PAN-OS Web Interface Help

Version 10.0

paloaltonetworks.com/documentation

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal www.paloaltonetworks.com/documentation.
- To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

December 18, 2020

Table of Contents

Web Interface Basics

The following topics provide an overview of the firewall and describes basic administrative tasks.

- Firewall Overview
- Features and Benefits
- Last Login Time and Failed Login Attempts
- Message of the Day
- Task Manager
- Language
- Alarms
- Commit Changes
- Save Candidate Configurations
- Revert Changes
- Lock Configurations
- Global Find
- Threat Details
- AutoFocus Intelligence Summary

Firewall Overview

Palo Alto Networks® next-generation firewalls inspect all traffic (including applications, threats, and content), and tie that traffic to the user, regardless of location or device type. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. This allows you to align security with your business policies, as well as write rules that are easy to understand and maintain.

As part of our Security Operating Platform, our next-generation firewalls provide your organization with the ability to:

- Securely enable applications (including software-as-a-service applications), users, and content by classifying all traffic (regardless of port).
- Reduce risk of an attack using a positive enforcement model, by allowing all desired applications and blocking everything else.
- Apply security policies to block known vulnerability exploits, viruses, ransomware, spyware, botnets, and other unknown malware, such as advanced persistent threats.
- Protect your data centers (including virtualized data centers) by segmenting data and applications, as well as enforcing the Zero Trust principle.
- Apply consistent security across your on-premises and cloud environments.
- Embrace secure mobile computing by extending the Security Operating Platform to users and devices, no matter where they are located.
- Get centralized visibility and streamline network security, making your data actionable so you can prevent successful cyberattacks.
- Identify and prevent attempts to steal credentials by stopping the submission of valid corporate credentials to illegitimate websites, and neutralizing an attacker's ability to use stolen credentials for lateral movement or network compromise by enforcing authentication policies at the network layer.

Features and Benefits

The Palo Alto Networks next-generation firewalls provide granular control over the traffic allowed to access your network. The primary features and benefits include:

- **Application-based policy enforcement (App-ID™)**—Access control according to application type is far more effective when application identification is based on more than just protocol and port number. The App-ID service can block high risk applications, as well as high risk behavior, such as file-sharing, and traffic encrypted with the Secure Sockets Layer (SSL) protocol can be decrypted and inspected.
- **User identification (User-ID™)**—The User-ID feature allows administrators to configure and enforce firewall policies based on users and user groups instead of or in addition to network zones and addresses. The firewall can communicate with many directory servers, such as Microsoft Active Directory, eDirectory, SunOne, OpenLDAP, and most other LDAP-based directory servers to provide user and group information to the firewall. You can then use this information for secure application enablement that can be defined per user or group. For example, the administrator could allow one organization to use a web-based application but not allow any other organizations in the company to use that same application. You can also configure granular control of certain components of an application based on users and groups (see User Identification).
- **Threat prevention**—Threat prevention services that protect the network from viruses, worms, spyware, and other malicious traffic can be varied by application and traffic source (see Objects > Security Profiles).
- **URL filtering**—Outbound connections can be filtered to prevent access to inappropriate web sites (see Objects > Security Profiles > URL Filtering).
- **Traffic visibility**—Extensive reports, logs, and notification mechanisms provide detailed visibility into network application traffic and security events. The Application Command Center (ACC) in the web interface identifies the applications with the most traffic and the highest security risk (see Monitor).
- **Networking versatility and speed**—The Palo Alto Networks firewall can augment or replace your existing firewall and can be installed transparently in any network or configured to support a switched or routed environment. Multigigabit speeds and a single-pass architecture provide these services to you with little or no impact on network latency.
- **GlobalProtect**—The GlobalProtect™ software provides security for client systems, such as laptops that are used in the field, by allowing easy and secure login from anywhere in the world.
- **Fail-safe operation**—High availability (HA) support provides automatic failover in the event of any hardware or software disruption (see Device > Virtual Systems).
- **Malware analysis and reporting**—The WildFire™ cloud-based analysis service provides detailed analysis and reporting on malware that passes through the firewall. Integration with the AutoFocus™ threat intelligence service allows you to assess the risk associated with your network traffic at organization, industry, and global levels.
- **VM-Series firewall**—A VM-Series firewall provides a virtual instance of PAN-OS® positioned for use in a virtualized data center environment and is ideal for your private, public, and hybrid cloud computing environments.
- **Management and Panorama**—You can manage each firewall through an intuitive web interface or through a command-line interface (CLI) or you can centrally manage all firewalls through the Panorama™ centralized management system, which has a web interface very similar to the web interface on Palo Alto Networks firewalls.

Last Login Time and Failed Login Attempts

To detect misuse and prevent exploitation of a privileged account, such as an administrative account on a Palo Alto Networks firewall or Panorama, the web interface and the command line interface (CLI) displays your last login time and any failed login attempts for your username when you log in. This information allows you to easily identify whether someone is using your administrative credentials to launch an attack.

After you log in to the web interface, the last login time information appears at the bottom left of the window. If one or more failed logins occurred since the last successful login, a caution icon appears to the right of the last login information. Hover over the caution symbol to view the number of failed login attempts or click to view the **Failed Login Attempts Summary** window, which lists the administrative account name, the source IP address, and the reason for the login failure.

If you see multiple failed login attempts that you do not recognize as your own, you should work with your network administrator to locate the system that is performing the brute-force attack and then investigate the user and host computer to identify and eradicate any malicious activity. If you see that the last login date and time indicates an account compromise, you should immediately change your password and then perform a configuration audit to determine if suspicious configuration changes were committed. Revert the configuration to a known good configuration if you see that logs were cleared or if you have difficulty determining if improper changes were made using your account.

Message of the Day

If you or another administrator configured a message of the day or Palo Alto Networks embedded one as part of a software or content release, a Message of the Day dialog displays automatically when users log in to the web interface. This ensures that users see important information, such as an impending system restart, that impacts the tasks they intend to perform.

The dialog displays one message per page. If the dialog includes the option to select **Do not show again**, you can select it for each message that you don't want the dialog to display after subsequent logins.

Anytime the Message of the Day changes, the message appears in your next session even if you selected Do not show again during a previous login. You must then reselect this option to avoid seeing the modified message in subsequent sessions.

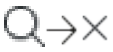
To navigate the dialog pages, click the right ( ) and left ( ) arrows along the sides of the dialog or click a page selector ( ) along the bottom of the dialog. After you **Close** the dialog, you can manually reopen it by clicking messages ( ) at the bottom of the web interface.

To configure a message of the day, select **Device** > **Setup** > **Management** and edit the Banners and Messages settings.

Task Manager

Click **Tasks** at the bottom of the web interface to display the tasks that you, other administrators, or PAN#OS initiated since the last firewall reboot (for example, manual commits or automatic FQDN refreshes). For each task, the Task Manager provides the information and actions described in the table below.

Some columns are hidden by default. To display or hide specific columns, open the drop-down in any column header, select Columns, and select (display) or clear (hide) the column names.

Field/Button	Description
	To filter the tasks, enter a text string based on a value in one of the columns and Apply Filter (→). For example, entering **`edl`** will filter the list to display only EDLFetch (fetch external dynamic lists) tasks. To remove filtering, Remove Filter (×).
Type	The type of task, such as log request, license refresh, or commit. If the information related to the task (such as warnings) is too long to fit in the Messages column, you can click the Type value to see all the details.
Status	Indicates whether the task is pending (such as commits with Queued status), in progress (such as log requests with Active status), completed, or failed. For commits in progress, the Status indicates the percentage of completion.
Job ID	A number that identifies the task. From the CLI, you can use the Job ID to see additional details about a task. For example, you can see the position of a commit task in the commit queue by entering: `> show jobs id <job-id>` This column is hidden by default.
End Time	The date and time when the task finished. This column is hidden by default.
Start Time	The date and time when the task started. For commit tasks, the Start Time indicates when the commit was added to the commit queue.
Messages	Displays details about the task. If the entry indicates that there are too many messages, you can click the task Type to see the messages. For commit tasks, the Messages include the dequeued time to indicate when PAN-OS started performing the commit. To see the description an administrator entered for a commit, click **Commit Description**. For details, see Commit Changes.

Field/Button	Description
Action	Click **x** to cancel a pending commit initiated by an administrator or PAN-OS. This button is available only to administrators who have one of the following predefined roles: superuser, device administrator, virtual system administrator, or Panorama administrator.
Show	Select the tasks you want to display: • **All Tasks** (default) • **All** tasks of a certain type (**Jobs**, **Reports**, or **Log Requests**) • All **Running** tasks (in progress) • All **Running** tasks of a certain type (**Jobs**, **Reports**, or **Log Requests**) • (Panorama only) Use the second drop-down to display the tasks for **Panorama** (default) or a specific managed firewall.
Clear Commit Queue	Cancel all pending commits initiated by administrators or PAN-OS. This button is available only to administrators who have one of the following predefined roles: superuser, device administrator, virtual system administrator, or Panorama administrator.

Language

By default, the language that is set on the computer used to log in to the firewall determines the language that is displayed on the management web interface. To manually change the language, click **Language** (bottom right of the web interface), select the desired language from the drop-down and click **OK**. The web interface refreshes and displays the web interface in the selected language.

Supported languages include: French, Japanese, Spanish, Simplified Chinese, and Traditional Chinese.

Alarms

An alarm is a firewall-generated message indicating that the number of events of a particular type (for example, encryption and decryption failures) has exceeded the threshold configured for that event type (see Define Alarm Settings). When generating an alarm, the firewall creates an Alarm log and opens the System Alarms dialog to display the alarm. After closing the dialog, you can reopen it anytime by clicking **Alarms** (

) at the bottom of the web interface. To prevent the firewall from automatically opening the dialog for a particular alarm, select Unacknowledged Alarms and click **Acknowledge** to move the alarms to the Acknowledged Alarms list.

Commit Changes

Click **Commit** at the top right of the web interface and specify an operation for pending changes to the firewall configuration: commit (activate), validate, or preview. You can filter pending changes by administrator or *location* and then preview, validate, and commit only those changes. The location can be specific virtual systems, shared policies and objects, or shared device and network settings.

The firewall queues commit requests so that you can initiate a new commit while a previous commit is in progress. The firewall performs the commits in the order they are initiated but prioritizes auto-commits that are initiated by the firewall (such as FQDN refreshes). However, if the queue already has the maximum number of administrator-initiated commits, you must wait for the firewall to finish processing a pending commit before initiating a new one.

Use the Task Manager to cancel commits or see details about commits that are pending, in progress, completed, or failed.

The Commit dialog displays the options described in the following table.

Field/Button	Description
Commit All Changes	Commits all changes for which you have administrative privileges (default). You cannot manually filter the scope of the configuration changes that the firewall commits when you select this option. Instead, the administrator role assigned to the account you used to log in determines the commit scope: • **Superuser role**—The firewall commits the changes of all administrators. • **Custom role**—The privileges of the Admin Role profile assigned to your account determine the commit scope (see Device > Admin Roles). If the profile includes the privilege to **Commit For Other Admins**, the firewall commits changes configured by any and all administrators. If your Admin Role profile does not include the privilege to **Commit For Other Admins**, the firewall commits only your changes and not those of other administrators. If you have implemented access domains, the firewall automatically applies those domains to filter the commit scope (see Device > Access Domain). Regardless of your administrative role, the firewall commits only the configuration changes in the access domains assigned to your account.
Commit Changes Made By	Filters the scope of the configuration changes the firewall commits. The administrative role assigned to the account you used to log in determines your filtering options: • **Superuser role**—You can limit the commit scope to changes that specific administrators made and to changes in specific locations. • **Custom role**—The privileges of the Admin Role profile assigned to your account determine your filtering options (see Device > Admin Roles). If the profile includes the privilege to **Commit For Other Admins**, you can limit the commit scope to changes configured by specific administrators and to changes in specific locations. If your Admin Role profile does not include the privilege to **Commit For**

Field/Button	Description
	Other Admins, you can limit the commit scope only to the changes you made in specific locations. Filter the commit scope as follows: • **Filter by administrator**—Even if your role allows committing the changes of other administrators, the commit scope includes only your changes by default. To add other administrators to the commit scope, click the **<usernames>** link, select the administrators, and click **OK**. • **Filter by location**—Select the specific locations for changes to Include in Commit. If you have implemented access domains, the firewall automatically filters the commit scope based on those domains (see Device > Access Domain). Regardless of your administrative role and your filtering choices, the commit scope includes only the configuration changes in the access domains assigned to your account. *After you load a configuration (Device > Setup > Operations), you must Commit All Changes.* When you commit changes to a virtual system, you must include the changes of all administrators who added, deleted, or repositioned rules for the same rulebase in that virtual system.
Commit Scope	Lists the locations that have changes to commit. Whether the list includes all changes or a subset of the changes depends on several factors, as described for Commit All Changes and Commit Changes Made By. The locations can be any of the following: • **shared-object**—Settings that are defined in the Shared location. • **policy-and-objects**—Policy rules or objects that are defined on a firewall that does not have multiple virtual systems. • **device-and-network**—Network and device settings that are global (such as Interface Management profiles) and not specific to a virtual system. This also applies to network and device settings on a firewall that does not have multiple virtual systems. • **<virtual-system>**—The name of the virtual system in which policy rules or objects are defined on a firewall that has multiple virtual systems. This also includes network and device settings that are specific to a virtual system (such as zones).
Location Type	This column categorizes the locations of pending changes: • **Virtual Systems**—Settings that are defined in a specific virtual system. • **Other Changes**—Settings that are not specific to a virtual system (such as shared objects).
Include in Commit (Partial commit only)	Enables you to select the changes you want to commit. By default, all changes within the **Commit Scope** are selected. This column displays only after you choose to **Commit Changes Made By** specific administrators.

Field/Button	Description
	There might be dependencies that affect the changes you include in a commit. For example, if you add an object and another administrator then edits that object, you cannot commit the change for the other administrator without also committing your own change.
Group by Location Type	Groups the list of configuration changes in the **Commit Scope** by **Location Type**.
Preview Changes	Enables you to compare the configurations you selected in the **Commit Scope** to the running configuration. The preview window uses color coding to indicate which changes are additions (green), modifications (yellow), or deletions (red). To help you match the changes to sections of the web interface, you can configure the preview window to display **Lines of Context** before and after each change. These lines are from the files of the candidate and running configurations that you are comparing. *Because the preview results display in a new browser window, your browser must allow pop-ups. If the preview window does not open, refer to your browser documentation for the steps to allow pop-ups.*
Change Summary	Lists the individual settings for which you are committing changes. The **Change Summary** list displays the following information for each setting: • **Object Name**—The name that identifies the policy, object, network setting, or device setting. • **Type**—The type of setting (such as Address, Security rule, or Zone). • **Location Type**—Indicates whether the setting is defined in **Virtual Systems**. • **Location**—The name of the virtual system where the setting is defined. The column displays **Shared** for settings that are not specific to a virtual system. • **Operations**—Indicates every operation (create, edit, or delete) performed on the setting since the last commit. • **Owner**—The administrator who made the last change to the setting. • **Will Be Committed**—Indicates whether the commit currently includes the setting. • **Previous Owners**—Administrators who made changes to the setting before the last change. Optionally, you can **Group By** column name (such as **Type**). Select an object in the change list to view the **Object Level Difference**.
Validate Commit	Validates whether the firewall configuration has correct syntax and is semantically complete. The output includes the same errors and

Field/Button	Description
	warnings that a commit would display, including rule shadowing and application dependency warnings. The validation process enables you to find and fix errors before you commit (it makes no changes to the running configuration). This is useful if you have a fixed commit window and want to be sure the commit will succeed without errors.
Description	Allows you to enter a description (up to 512 characters) to help other administrators understand what changes you made.  *The System log for a commit event will truncate descriptions longer than 512 characters.*
Commit	Starts the commit or, if other commits are pending, adds your commit to the commit queue.
Commit Status	Provides progress during the commit, then provides results after the commit. Commit results include success or failure, details of commit changes, and commit warnings. Warnings include: • **Commit**—Lists general commit warnings. • **App Dependency**—Lists any app dependencies required for existing rules. • **Rule Shadow**—Lists any shadow rules.

Save Candidate Configurations

Select **Config** > **Save Changes** at the top right of the firewall or Panorama web interface to save a new snapshot file of the candidate configuration or to overwrite an existing configuration file. If the firewall or Panorama reboots before you commit your changes, you can then revert the candidate configuration to the saved snapshot to restore changes you made after the last commit. To revert to the snapshot, select **Device** > **Setup** > **Operations** and **Load named configuration snapshot**. If you don't revert to the snapshot after a reboot, the candidate configuration will be the same as the last committed configuration (the running configuration).

You can filter which configuration changes to save based on administrator or *location*. The location can be specific virtual systems, shared policies and objects, or shared device and network settings.

You should periodically save your changes so that you don't lose them if the firewall or Panorama reboots.

Saving your changes to the candidate configuration does not activate those changes; you must Commit Changes to activate them.

The Save Changes dialog displays the options described in the following table:

Field/Button	Description
Save All Changes	Saves all changes for which you have administrative privileges (default). You cannot manually filter the scope of the configuration changes that the firewall saves when you select this option. Instead, the administrator role assigned to the account you used to log in determines the save scope: • **Superuser role**—The firewall saves the changes of all administrators. • **Custom role**—The privileges of the Admin Role profile assigned to your account determine the save scope (see Device > Admin Roles). If the profile includes the privilege to **Save For Other Admins**, the firewall saves changes configured by any and all administrators. If your Admin Role profile does not include the privilege to **Save For Other Admins**, the firewall saves only your changes and not those of other administrators. If you have implemented access domains, the firewall automatically applies those domains to filter the save scope (see Device > Access Domain). Regardless of your administrative role, the firewall saves only the configuration changes in the access domains assigned to your account.
Save Changes Made By	Filters the scope of the configuration changes the firewall saves. The administrative role assigned to the account you used to log in determines your filtering options: • **Superuser role**—You can limit the save scope to changes that specific administrators made and to changes in specific locations. • **Custom role**—The privileges of the Admin Role profile assigned to your account determine your filtering options (see Device >

Field/Button	Description
	Admin Roles). If the profile includes the privilege to **Save For Other Admins**, you can limit the save scope to changes configured by specific administrators and to changes in specific locations. If your Admin Role profile does not include the privilege to **Save For Other Admins**, you can limit the save scope only to the changes you made in specific locations. Filter the save scope as follows: • **Filter by administrator**—Even if your role allows saving the changes of other administrators, the save scope includes only your changes by default. To add other administrators to the save scope, click the **<usernames>** link, select the administrators, and click **OK**. • **Filter by location**—Select changes in specific locations to Include in Save. If you have implemented access domains, the firewall automatically filters the save scope based on those domains (see Device > Access Domain). Regardless of your administrative role and your filtering choices, the save scope includes only the configuration changes in the access domains assigned to your account.
Save Scope	Lists the locations that have changes to save. Whether the list includes all changes or a subset of the changes depends on several factors, as described for the Save All Changes and Save Changes Made By options. The locations can be any of the following: • **shared-object**—Settings that are defined in the Shared location. • **policy-and-objects**—(Firewall only) Policy rules or objects that are defined on a firewall that does not have multiple virtual systems. • **device-and-network**—(Firewall only) Network and device settings that are global (such as Interface Management profiles) and not specific to a virtual system. • **<virtual-system>**—(Firewall only) The name of the virtual system in which policy rules or objects are defined on a firewall that has multiple virtual systems. This also includes network and device settings that are specific to a virtual system (such as zones). • **<device-group>**—(Panorama only) The name of the device group in which the policy rules or objects are defined. • **<template>**—(Panorama only) The name of the template or template stack in which the settings are defined. • **<log-collector-group>**—(Panorama only) The name of the Collector Group in which the settings are defined. • **<log-collector>**—(Panorama only) The name of the Log Collector in which the settings are defined.
Location Type	This column categorizes the locations where the changes were made: • **Virtual Systems**—(Firewall only) Settings that are defined in a specific virtual system. • **Device Groups**—(Panorama only) Settings that are defined in a specific device group. • **Templates**—(Panorama only) Settings that are defined in a specific template or template stack.

Field/Button	Description
	• **Collector Groups**—(Panorama only) Settings that are specific to a Collector Group configuration.
Include in Save (Partial save only)	Enables you to select the changes you want to save. By default, all changes within the **Save Scope** are selected. This column displays only after you choose to **Save Changes Made By** specific administrators.  *There might be dependencies that affect the changes you include in a save. For example, if you add an object and another administrator then edits that object, you cannot save the change for the other administrator without also saving your own change.*
Group by Location Type	Groups the list of configuration changes in the **Save Scope** by **Location Type**.
Preview Changes	Enables you to compare the configurations you selected in the **Save Scope** to the running configuration. The preview window uses color coding to indicate which changes are additions (green), modifications (yellow), or deletions (red). To help you match the changes to sections of the web interface, you can configure the preview window to display **Lines of Context** before and after each change. These lines are from the files of the candidate and running configurations that you are comparing.  *Because the preview results display in a new window, your browser must allow pop-up windows. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-up windows.*
Change Summary	Lists the individual settings for which you are saving changes. The **Change Summary** list displays the following information for each setting: • **Object Name**—The name that identifies the policy, object, network setting, or device setting. • **Type**—The type of setting (such as Address, Security rule, or Zone). • **Location Type**—Indicates whether the setting is defined in **Virtual Systems**. • **Location**—The name of the virtual system where the setting is defined. The column displays **Shared** for settings that are not specific to a virtual system. • **Operations**—Indicates every operation (create, edit, or delete) performed on the setting since the last commit. • **Owner**—The administrator who made the last change to the setting. • **Will Be Saved**—Indicates whether the save operation will include the setting. • **Previous Owners**—Administrators who made changes to the setting before the last change.

Field/Button	Description
	Optionally, you can **Group By** column name (such as **Type**).
Save	Saves the selected changes to a configuration snapshot file: • If you selected **Save All Changes**, the firewall overwrites the default configuration snapshot file (.snapshot.xml). • If you selected **Save Changes Made By**, specify the **Name** of a new or existing configuration file, and click **OK**.

Revert Changes

Select **Config** > **Revert Changes** at the top right of the firewall or Panorama web interface to undo changes made to the candidate configuration since the last commit. Reverting changes restores the settings to the values of the running configuration. You can filter which configuration changes to revert based on administrator or *location*. The location can be specific virtual systems, shared policies and objects, or shared device and network settings.

You cannot revert changes until the firewall or Panorama finishes processing all commits that are pending or in progress. After you initiate the revert process, the firewall or Panorama automatically locks the candidate and running configurations so that other administrators cannot edit settings or commit changes. After completing the revert process, the firewall or Panorama automatically removes the lock.

The Revert Changes dialog displays the options described in the following table:

Field/Button	Description
Revert All Changes	Reverts all changes for which you have administrative privileges (default). You cannot manually filter the scope of the configuration changes that the firewall reverts when you select this option. Instead, the administrator role assigned to the account you used to log in determines the revert scope: • **Superuser role**—The firewall reverts the changes of all administrators. • **Custom role**—The privileges of the Admin Role profile assigned to your account determine the revert scope (see Device > Admin Roles). If the profile includes the privilege to **Commit For Other Admins**, the firewall reverts changes configured by any and all administrators. If your Admin Role profile does not include the privilege to **Commit For Other Admins**, the firewall reverts only your changes and not those of other administrators.  *In Admin Role profiles, the privileges for committing also apply to reverting.* If you implemented access domains, the firewall automatically applies those domains to filter the revert scope (see Device > Access Domain). Regardless of your administrative role, the firewall reverts only the configuration changes in the access domains assigned to your account.
Revert Changes Made By	Filters the scope of configuration changes that the firewall reverts. The administrative role assigned to the account you used to log in determines your filtering options: • **Superuser role**—You can limit the revert scope to changes that specific administrators made and to changes in specific locations. • **Custom role**—The privileges of the Admin Role profile assigned to your account determine your filtering options (see Device > Admin Roles). If the profile includes the privilege to **Commit For Other Admins**, you can limit the revert scope to changes configured by specific administrators and to changes in specific locations. If your Admin Role profile does not include the privilege to **Commit For**

Field/Button	Description
	Other Admins, you can limit the revert scope only to the changes you made in specific locations. Filter the revert scope as follows: • **Filter by administrator**—Even if your role allows reverting the changes of other administrators, the revert scope includes only your changes by default. To add other administrators to the revert scope, click the **<usernames>** link, select the administrators, and click **OK**. • **Filter by location**—Select the changes in specific locations to Include in Revert. If you have implemented access domains, the firewall automatically filters the revert scope based on those domains (see Device > Access Domain). Regardless of your administrative role and your filtering choices, the revert scope includes only the configuration changes in the access domains assigned to your account.
Revert Scope	Lists the locations that have changes to revert. Whether the list includes all changes or a subset of the changes depends on several factors, as described for the Revert All Changes and Revert Changes Made By options. The locations can be any of the following: • **shared-object**—Settings that are defined in the Shared location. • **policy-and-objects**—(Firewall only) Policy rules or objects that are defined on a firewall that does not have multiple virtual systems. • **device-and-network**—(Firewall only) Network and device settings that are global (such as Interface Management profiles) and not specific to a virtual system. • **<virtual-system>**—(Firewall only) The name of the virtual system in which policy rules or objects are defined on a firewall that has multiple virtual systems. This also includes network and device settings that are specific to a virtual system (such as zones). • **<device-group>**—(Panorama only) The name of the device group in which the policy rules or objects are defined. • **<template>**—(Panorama only) The name of the template or template stack in which the settings are defined. • **<log-collector-group>**—(Panorama only) The name of the Collector Group in which the settings are defined. • **<log-collector>**—(Panorama only) The name of the Log Collector in which the settings are defined.
Location Type	This column categorizes the locations where the changes were made: • **Virtual Systems**—(Firewall only) Settings that are defined in a specific virtual system. • **Device Group**—(Panorama only) Settings that are defined in a specific device group. • **Template**—(Panorama only) Settings that are defined in a specific template or template stack. • **Log Collector Group**—(Panorama only) Settings that are specific to a Collector Group configuration.

Field/Button	Description
	• **Log Collector**—(Panorama only) Settings that are specific to a Log Collector configuration. • **Other Changes**—Settings that are not specific to any of the preceding configuration areas (such as shared objects).
Include in Revert (Partial revert only)	Enables you to select the changes you want to revert. By default, all changes within the **Revert Scope** are selected. This column displays only after you choose to **Revert Changes Made By** specific administrators.  *There might be dependencies that affect the changes you include in a revert. For example, if you add an object and another administrator then edits that object, you cannot revert your change without also reverting the change for the other administrator.*
Group by Location Type	Lists the configuration changes in the **Revert Scope** by **Location Type**.
Preview Changes	Enables you to compare the configurations you selected in the **Revert Scope** to the running configuration. The preview window uses color coding to indicate which changes are additions (green), modifications (yellow), or deletions (red). To help you match the changes to sections of the web interface, you can configure the preview window to display **Lines of Context** before and after each change. These lines are from the files of the candidate and running configurations that you are comparing.  *Because the preview results display in a new window, your browser must allow pop-up windows. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-up windows.*
Change Summary	Lists the individual settings for which you are reverting changes. The **Change Summary** list displays the following information for each setting: • **Object Name**—The name that identifies the policy, object, network setting, or device setting. • **Type**—The type of setting (such as Address, Security rule, or Zone). • **Location Type**—Indicates whether the setting is defined in **Virtual Systems**. • **Location**—The name of the virtual system where the setting is defined. The column displays **Shared** for settings that are not specific to a virtual system. • **Operations**—Indicates every operation (create, edit, or delete) performed on the setting since the last commit. • **Owner**—The administrator who made the last change to the setting. • **Will Be Reverted**—Indicates whether the revert operation will include the setting.

Field/Button	Description
	• **Previous Owners**—Administrators who made changes to the setting before the last change. Optionally, you can **Group By** column name (such as **Type**).
Revert	Reverts the selected changes.

Lock Configurations

To help you coordinate configuration tasks with other firewall administrators during concurrent login sessions, the web interface enables you to apply a configuration or commit lock so that other administrators cannot change the configuration or commit changes until the lock is removed.

At the top right of the web interface, a locked padlock ( ) indicates that one or more locks are set (with the number of locks in parentheses); an unlocked padlock ( ) indicates that no locks are set. Clicking either padlock opens the Locks dialog, which provides the following options and fields.

To configure the firewall to automatically set a commit lock whenever an administrator changes the candidate configuration, select Device > Setup > Management, edit the General Settings, enable Automatically Acquire Commit Lock, and then click OK and Commit.

When you revert changes (Config > Revert Changes), the firewall automatically locks the candidate and running configuration so that other administrators cannot edit settings or commit changes. After completing the revert process, the firewall automatically removes the lock.

Field/Button	Description
Admin	The username of the administrator who set the lock.
Location	On a firewall with more than one virtual system (vsys), the scope of the lock can be a specific vsys or the Shared location.
Type	The lock type can be: • **Config Lock**—Blocks other administrators from changing the candidate configuration. Only a superuser or the administrator who set the lock can remove it. • **Commit Lock**—Blocks other administrators from committing changes made to the candidate configuration. The commit queue does not accept new commits until all locks are released. This lock prevents collisions that can occur when multiple administrators make changes during concurrent login sessions and one administrator finishes and initiates a commit before the other administrators have finished. The firewall automatically removes the lock after completing the commit for which the administrator set the lock. A superuser or the administrator who set the lock can also manually remove it.
Comment	Enter up to 256 characters of text. This is useful for other administrators who want to know the reason for the lock.
Created At	The date and time when an administrator set the lock.
Logged In	Indicates whether the administrator who set the lock is currently logged in.

Field/Button	Description
Take a Lock	To set a lock, **Take a Lock**, select the **Type**, select the **Location** (multiple virtual system firewalls only), enter optional **Comments**, click **OK**, and then **Close**.
Remove Lock	To release a lock, select it, **Remove Lock**, click **OK**, and then **Close**.

Global Find

Global Find enables you to search the candidate configuration on a firewall or on Panorama for a particular string, such as an IP address, object name, policy name, threat ID, rule UUID, or application name. The search results are grouped by category and provide links to the configuration location in the web interface so that you can easily find all of the places where the string exists or is referenced.

To launch global find, click the **Search** icon  on the upper right side of the web interface. Global Find is available from all web interface pages and locations. The following is a list of Global Find features to help you perform successful searches:

- If you initiate a search on a firewall that has multiple virtual systems enabled or if administrative roles are defined, Global Find will return results only for areas of the firewall for which you have permission to access. The same applies to Panorama device groups; you will see search results only for device groups to which you have administrative access.
- Spaces in search text are handled as AND operations. For example, if you search on **`corp policy`**, both **corp** and **policy** must exist in the configuration item for it to be included in the search results.
- To find an exact phrase, surround the phrase in quotes.
- To re-run a previous search, click Global Find and a list of the last 20 searches are displayed. Click any item in the list to re-run that search. The search history list is unique to each administrative account.

Global Find is available for each field that is searchable. For example, in the case of a Security policy, you can search on the following fields: Name, Tags, Zone, Address, User, HIP Profile, Application, UUID, and Service. To perform a search, click the drop-down next to any of these fields and click **Global Find**. For example, if you click **Global Find** on a zone named l3-vlan-trust, Global Find will search the entire configuration for that zone name and return results for each location where the zone is referenced. The search results are grouped by category and you can hover over any item to view details or you can click an item to navigate to the configuration page for that item.

Global Find does not search dynamic content that the firewall allocates to users (such as logs, address ranges, or individual DHCP addresses). In the case of DHCP, you can search on a DHCP server attribute, such as the DNS entry, but you cannot search for individual addresses issued to users. Another example is usernames that the firewall collects when you enable the User-ID™ feature. In this case, a username or user group that exists in the User-ID database is only searchable if the name or group exists in the configuration, such as when a user group name is defined in a policy. In general, you can only search for content that the firewall writes to the configuration.

Looking for more?

Learn more about using Global Find to search the firewall or Panorama configuration.

Threat Details

- Monitor > Logs > Threat
- ACC > Threat Activity
- Objects > Security Profiles > Anti-Spyware/Vulnerability Protection

Use the Threat Details dialog to learn more about the threat signatures with which the firewall is equipped and the events that trigger those signatures. Threat details are provided for:

- Threat logs that record the threats that the firewall detects (**Monitor** > **Logs** > **Threat**)
- The top threats found in your network (**ACC** > **Threat Activity**)
- Threat signatures that you want to modify or exclude from enforcement (**Objects** > **Security Profiles** > **Anti-Spyware/Vulnerability Protection**)

When you find a threat signature you want to learn more about, hover over the **Threat Name** or the threat **ID** and click **Exception** to review the threat details. The threat details allow you to easily check whether a threat signature is configured as an exception to your security policy and to find the latest Threat Vault information about a specific threat. The Palo Alto Networks Threat Vault database is integrated with the firewall, allowing you to view expanded details about threat signatures in the firewall context or launch a Threat Vault search in a new browser window for a logged threat.

Depending on the type of threat you're viewing, the details include all or some of the threat details described in the following table.

Threat Details	Description
Name	Threat signature name.
ID	Unique threat signature ID. Select **View in Threat Vault** to open a Threat Vault search in a new browser window and look up the latest information that the Palo Alto Networks threat database has for this signature. The Threat Vault entry for the threat signature might include additional details, including the first and last content releases to include updates to the signature and the minimum PAN-OS version required to support the signature.
Description	Information about the threat that triggers the signature.
Severity	The threat severity level: informational, low, medium, high, or critical.
CVE	Publicly known security vulnerabilities associated with the threat. The Common Vulnerabilities and Exposures (CVE) identifier is the most useful identifier for finding information about unique vulnerabilities as vendor-specific IDs commonly encompass multiple vulnerabilities.
Bugtraq ID	The Bugtraq ID associated with the threat.
Vendor ID	The vendor-specific identifier for a vulnerability. For example, MS16-148 is the vendor ID for one or more Microsoft vulnerabilities and APBSB16-39 is the vendor ID for one or more Adobe vulnerabilities.
Reference	Research sources you can use to learn more about the threat.

Threat Details	Description
Exempt Profiles	Security profiles that define a different enforcement action for the threat signature than the default signature action. The threat exception is only active when exempt profiles are attached to a security policy rule (check if the exception is Used in current security rule).
Used in current security rule	Active threat exceptions—A check mark in this column indicates that the firewall is actively enforcing the threat exception (the Exempt Profiles that define the threat exception are attached to a security policy rule). If this column is clear, the firewall is enforcing the threat based only on the recommended default signature action.
Exempt IP Addresses	Exempt IP addresses—You can add an IP address on which to filter the threat exception or view existing **Exempt IP Addresses**. This option enforces a threat exception only when the associated session has either a source or destination IP address that matches the exempt IP address. For all other sessions, the threat is enforced based on the default signature action.

If you're having trouble viewing threat details, check for the following conditions:

- *The firewall Threat Prevention license is active (Device > Licenses).*
- *The latest Antivirus and Threats and Applications content updates are installed.*
- *Threat Vault access is enabled (select Device > Setup > Management and edit the Logging and Reporting setting to Enable Threat Vault Access).*
- *The default (or custom)* Antivirus, Anti-Spyware, and Vulnerability Protection security profiles *are applied to your security policy.*

AutoFocus Intelligence Summary

You can view a graphical overview of threat intelligence that AutoFocus compiles to help you assess the pervasiveness and risk of the following firewall artifacts:

- IP Address
- URL
- Domain
- User agent (found in the User Agent column of Data Filtering logs)
- Threat name (only for threats of the subtypes virus and wildfire-virus)
- Filename
- SHA-256 hash (found in the File Digest column of WildFire Submissions logs)

To view the AutoFocus Intelligence Summary window, you must first have an active AutoFocus subscription and enable AutoFocus threat intelligence (select **Device** > **Setup** > **Management** and edit the AutoFocus settings).

After you've enabled AutoFocus intelligence, hover over a log or external dynamic list artifact to open the drop-down ( ) and then click **AutoFocus**:

- View Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, and Unified logs (**Monitor** > **Logs**).
- View external dynamic list entries.

You can also launch an AutoFocus search from the firewall, to further investigate interesting or suspicious artifacts that you find.

Field/Button	Description
Search AutoFocus for...	Click to launch an AutoFocus search for the artifact.
Analysis Information Tab	
Sessions	The number of private sessions in which WildFire detected the artifact. Private sessions are sessions running only on firewalls associated with your support account. Hover over a session bar to view the number of sessions per month.
Samples	Organization and global samples (files and email links) associated with the artifact and grouped by WildFire verdict (benign, grayware, malware, phishing). *Global* refers to samples from all WildFire submissions, while *organization* refers only to samples submitted to WildFire by your organization. Click on a WildFire verdict to launch an AutoFocus search for the artifact filtered by scope (organization or global) and WildFire verdict.
Matching Tags	AutoFocus tags matched to the artifact: • **Private Tags**—Visible only to AutoFocus users associated with your support account. • **Public Tags**—Visible to all AutoFocus users. • **Unit 42 Tags**—Identify threats and campaigns that pose a direct security risk. These tags are created by Unit 42 (the Palo Alto Networks threat intelligence and research team). • **Informational Tags**—Unit 42 tags that identify commodity threats.

Field/Button	Description
	Hover over a tag to view the tag description and other tag details. Click a tag to launch an AutoFocus search for that tag. To view more matching tags for an artifact, click the ellipsis (...) to launch an AutoFocus search for that artifact. The Tags column in the AutoFocus search results displays more matching tags for the artifact.
Passive DNS Tab The Passive DNS tab displays passive DNS history associated with the artifact. This tab only displays matching information if the artifact is an IP address, domain, or URL.	
Request	The domain that submitted a DNS request. Click the domain to launch an AutoFocus search for it.
Type	The DNS request type (example: A, NS, CNAME).
Response	The IP address or domain to which the DNS request resolved. Click the IP address or domain to launch an AutoFocus search. *The Response column does not display private IP addresses.*
Count	The number of times the request was made.
First Seen	The date and time that the Request, Response, and Type combination was first seen based on passive DNS history.
Last Seen	The date and time that the Request, Response, and Type combination was most recently seen based on passive DNS history.
Matching Hashes Tab The Matching Hashes tab displays the five most recent private samples where WildFire detected the artifact. Private samples are samples detected only on firewalls associated with your support account.	
SHA256	The SHA-256 hash for a sample. Click the hash to launch an AutoFocus search for that hash.
File Type	The file type of the sample.
Create Date	The date and time that WildFire analyzed a sample and assigned a WildFire verdict to it.
Update Date	The date and time that WildFire updated the WildFire verdict for a sample.
Verdict	The WildFire verdict for a sample: benign, grayware, malware, or phishing.

Configuration Table Export

Administrative users can export the data on policy rulebase, objects, managed devices, and interfaces in tabular format in either a PDF file or a CSV file. The data that is exported is the visible data on the web interface. For filtered data, only data matching the filter is exported. If you don't apply any filter, then all data is exported.

All sensitive data, such as a password, is hidden with wildcard (*) symbols.

A system log and download link are generated on successful configuration table export. Use the download link to save the PDF or CSV file locally. After you close the window that contains the download link, the download link for that specific export is no longer available.

To export table data, click **PDF/CSV** and configure the following settings:

Export Settings	Description
File Name	Enter a name (maximum of 32 characters) to identify the exported data. This name becomes the name of the downloaded file that is generated by the export.
File Type	Select the type of export output to generate. You can choose either PDF or CSV format.
Page Size	The default page size is Letter (8.5 by 11.0 inches). You cannot change the page size. By default, the PDF is generated in portrait orientation and changes to landscape orientation to accommodate the maximum number of columns.
Description (PDF only)	Enter a description (maximum of 255 characters) to provide context and additional information about the export.
Table Data	Shows the table data that will be exported. If you need to clear the filtering settings that you set previously, click **Show All Columns** to show all policy rules under the selected policy type. Then you can add or remove columns and apply filters as needed.
Show All Columns	Remove all filters and show all table columns.

Click **Export** to generate the configuration table download link.

Dashboard

The Dashboard widgets show general firewall or Panorama™ information, such as the software version, status of each interface, resource utilization, and up to 10 entries for each of several log types; log widgets display entries from the last hour.

The Dashboard Widgets topic describes how to use the Dashboard and describes the available widgets.

Dashboard Widgets

By default, the **Dashboard** displays widgets in a **Layout** of **3 Columns** but you can customize the **Dashboard** to display only **2 Columns**, instead.

You can also decide which widgets to display or hide so that you see only those you want to monitor. To display a widget, select a widget category from the **Widgets** drop-down and select a widget to add it to the Dashboard (widget names that appear in faded grayed-out text are already displayed). Hide (stop displaying) a widget by closing the widget ( in the widget header). The firewalls and Panorama save your widget display settings across logins (separately for each administrator).

Refer to the **Last updated** timestamp to determine when the Dashboard data was last refreshed. You can manually refresh the entire **Dashboard** ( in the top right corner of the Dashboard) or you can refresh individual widgets ( within each widget header). Use the unlabeled drop-down next to the manual Dashboard refresh option () to select the automatic refresh interval for the entire **Dashboard** (in minutes): **1 min**, **2 mins**, or **5 mins**; to disable automatic refresh for the entire **Dashboard**, select **Manual**.

Dashboard Widgets	Description
Application Widgets	
Top Applications	Displays the applications with the most sessions. The block size indicates the relative number of sessions (mouse over the block to view the number), and the color indicates the security risk—from green (lowest) to red (highest). Click an application to view its application profile.
Top High Risk Applications	Similar to Top Applications except that it displays the highest-risk applications with the most sessions.
ACC Risk Factor	Displays the average risk factor (1-5) for the network traffic processed over the past week. Higher values indicate higher risk.
System Widgets	
General Information	Displays the firewall or Panorama name and model, the Panorama CPU and RAM, the Panorama system mode, the PAN-OS® or Panorama software version, the IPv4 and IPv6 management IP information, the serial number, the CPU ID and UUID, the application, threat, and URL filtering definition versions, the current date and time, and the length of time since the last restart.
Interfaces (Firewall only)	Indicates whether each interface is up (green), down (red), or in an unknown state (gray).
System Resources	Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or Panorama).
High Availability	Indicates—when high availability (HA) is enabled—the HA status of the local and peer firewall/Panorama—green (active), yellow (passive), or black (other). For more information about HA, refer to Device > Virtual Systems or Panorama > High Availability.

Dashboard Widgets	Description
Locks	Shows configuration locks that administrators have set.
Logged In Admins	Displays the source IP address, session type (web interface or CLI), and session start time for each administrator who is currently logged in.
Logs Widgets	
Threat Logs	Displays the threat ID, application, and date and time for the last 10 entries in the Threat log. The threat ID is a malware description or URL that violates the URL filtering profile. Displays only entries from the last 60 minutes.
URL Filtering Logs	Displays the description and date and time for the last 60 minutes in the URL Filtering log.
Data Filtering Logs	Displays the description and date and time for the last 60 minutes in the Data Filtering log.
Config Logs	Displays the administrator username, client (web interface or CLI), and date and time for the last 10 entries in the Configuration log. Displays only entries from the last 60 minutes.
System Logs	Displays the description and date and time for the last 10 entries in the System log.  *A "Config installed" entry indicates configuration changes were committed successfully. Displays only entries from the last 60 minutes.*

ACC

The Application Command Center (ACC) is an analytical tool that provides actionable intelligence about the activity within your network. The ACC uses the firewall logs to graphically depict traffic trends on your network. The graphical representation allows you to interact with the data and visualize the relationships between events on the network including network usage patterns, traffic patterns, and suspicious activity and anomalies.

- A First Glance at the ACC
- ACC Tabs
- ACC Widgets
- ACC Actions
- Working with Tabs and Widgets
- Working with Filters—Local Filters and Global Filters

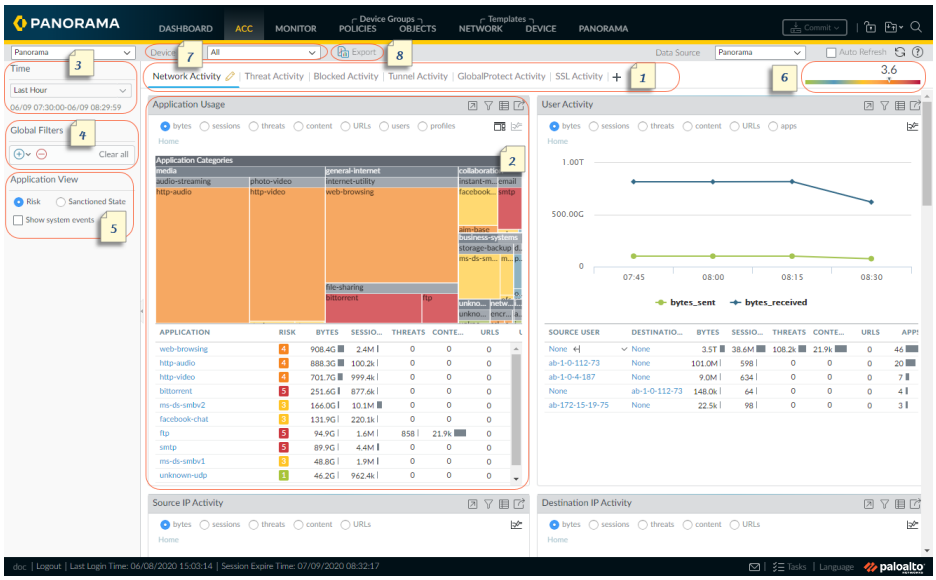
Looking for more?

See Use the Application Command Center.

A First Glance at the ACC

The following table shows the ACC tab and describes each component.

A First Glance at the ACC



1	**Tabs**	The ACC includes predefined tabs that provide visibility into network traffic, threat activity, blocked activity, tunnel activity, and mobile network activity (if GTP security is enabled). For information on each tab, see ACC Tabs.
2	**Widgets**	Each tab includes a default set of widgets that best represent the events and trends associated with the tab. The widgets allow you to survey the data using the following filters: bytes (in and out), sessions, content (files and data), URL categories, applications, users, threats (malicious, benign, grayware, phishing), and count. For information on each widget, see ACC Widgets.
3	**Time**	The charts and graphs in each widget provide a real-time and historic view. You can choose a custom range or use the predefined time periods that range from the last 15 minutes up to the last 90 days or last 30 calendar days. The time period used to render data, by default, is the last hour. The date and time interval are displayed on screen. For example: `11/11 10:30:00-01/12 11:29:59`
4	**Global Filters**	The global filters allow you to set the filter across all tabs. The charts and graphs apply the selected filters before rendering the data. For information on using the filters, see ACC Actions.
5	**Application View**	The application view allows you filter the ACC view by either the sanctioned and unsanctioned applications in use on your network, or by the risk level of the applications in use on your network. Green indicates sanctioned applications, blue

		unsanctioned applications, and yellow indicates applications that have different sanctioned state across different virtual systems or device groups.
6	**Risk Meter**	The risk meter (1=lowest to 5=highest) indicates the relative security risk on your network. The risk meter uses a variety of factors such as the type of applications seen on the network and the risk levels associated with the applications, the threat activity and malware as seen through the number of blocked threats, and compromised hosts or traffic to malware hosts and domains.
7	**Source**	The data used for the display varies between the firewall and Panorama™. You have the following options to select what data is used to generate the views on the ACC: **Virtual System**: On a firewall that is enabled for multiple virtual systems, you can use the **Virtual System** drop-down to change the ACC display to include all virtual systems or just a selected virtual system. **Device Group**: On Panorama, you can use the **Device Group** drop-down to change the ACC display to include data from all device groups or just a selected device group. **Data Source**: On Panorama, you can also change the display to use **Panorama** or **Remote Device Data** (managed firewall data). When the data source is **Panorama**, you can filter the display for a specific device group.
8	**Export**	You can export the widgets displayed in the current tab as a PDF.

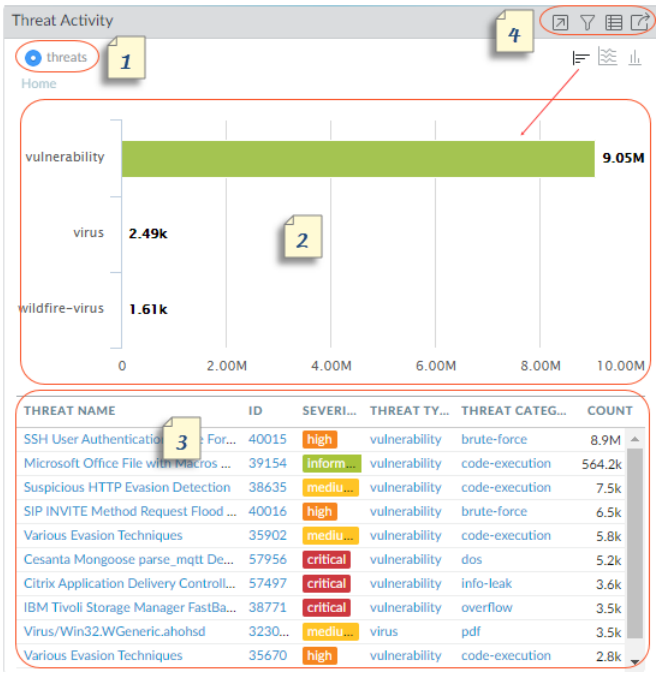
ACC Tabs

- **Network Activity**—Displays an overview of traffic and user activity on your network. This view focuses on the top most-used applications, the top users who generate traffic with a drill down into the bytes, content, threats, and URLs accessed by the user, and the most used Security policy rules against which traffic matches occur. In addition, you can view network activity by source or destination zone, region, or IP address; by ingress or egress interfaces; and by host information, such as the operating systems of the devices most commonly used on the network.
- **Threat Activity**—Displays an overview of the threats on the network. It focuses on the top threats—vulnerabilities, spyware, viruses, hosts visiting malicious domains or URLs, top WildFire submissions by file type and application, and applications that use non-standard ports. The Compromised Hosts widget supplements detection with better visualization techniques. It uses the information from the correlated events tab (Monitor > Automated Correlation Engine > Correlated Events) to present an aggregated view of compromised hosts on your network by source users or IP addresses, sorted on severity.
- **Blocked Activity**—Focuses on traffic that was prevented from coming into the network. The widgets in this tab allow you to view activity denied by application name, username, threat name, content (files and data), and the top security rules with a deny action that blocked traffic.
- **Mobile Network Activity**—Displays a visual representation of mobile traffic on your network using GTP logs generated from your Security policy rule configuration. This view includes interactive and customizable GTP Events, Mobile Subscriber Activity, and GTP Rejection Cause widgets to which you can apply ACC Filters and drill down to isolate the information you need. When you enable SCTP Security, widgets on this tab display a visual representation and details of SCTP events on the firewall, as well as the number of chunks sent and received per SCTP Association ID.
- **Tunnel Activity**—Displays the activity of tunnel traffic that the firewall inspected based on your tunnel inspection policies. Information includes tunnel usage based on tunnel ID, monitor tag, user, and tunnel protocols such as Generic Routing Encapsulation (GRE), General Packet Radio Service (GPRS) tunneling protocol for user data (GTP-U), and non-encrypted IPSec.
- **GlobalProtect Activity**—Displays an overview of user activity in your GlobalProtect deployment. Information includes the number of users and number of times users connected, the gateways to which users connected, the number of connection failures and the failure reason, a summary of authentication methods and GlobalProtect app versions used, and the number of endpoints that are quarantined.
- **SSL Activity**—Displays the activity of decrypted and undecrypted TLS/SSL traffic based on your Decryption policies and profiles. You can see TLS activity compared to non-TLS activity, the amount of decrypted traffic versus the amount of undecrypted traffic, reasons for decryption failures, and successful TLS version and key exchange activity. Use this information to identify traffic that causes decryption issues and then use the Decryption Log and custom Decryption report templates to drill down into details and gain context about that traffic so that you can diagnose and fix issues accurately.

You can also customize tabs and widgets as described in Working with Tabs and Widgets*.*

ACC Widgets

The widgets on each tab are interactive. You can set filters and drill down into the display to customize the view and focus on the information you need.



Each widget is structured to display the following information:

1	**View**	You can sort the data by bytes, sessions, threats, count, users, content, applications, URLs, malicious, benign, grayware, phishing, file(name)s, data, profiles, objects, portals, gateways, and profiles. The available options vary by widget.
2	**Graph**	The graphical display options are treemap, line graph, horizontal bar graph, stacked area graph, stacked bar graph, pie chart, and map. The available options vary by widget and the interaction experience varies with each graph type. For example, the widget for Applications using Non-Standard Ports allows you to choose between a treemap and a line graph. To drill down into the display, click on the graph. The area you click on becomes a filter and allows you to zoom in and view more granular information about that selection.
3	**Table**	The detailed view of the data used to render the graph displays in a table below the graph. You can click and set a local filter or a global filter for elements in the table. With a local filter, the graph is updated and the table is sorted by that filter. With a global filter, the view across the ACC pivots to display only the information specific to your filter.
4	**Actions**	The following are actions available in the title bar of a widget:

		• **Maximize view**—Allows you to enlarge the widget and view it in a larger screen space. In the maximized view, you can see more than the top ten items that display in the default widget view. • **Set up local filters**—Allows you to add filters that refine the display within the widget. See Working with Filters—Local Filters and Global Filters. • **Jump to logs**—Allows you to directly navigate to the logs (**Monitor** > **Logs** > **<log-type>**). The logs are filtered using the time period for which the graph is rendered. If you set local and global filters, the log query concatenates the time period and filters and displays only logs that match your filter set. • **Export**—Allows you to export the graph as a PDF.

For a description of each widget, see the details on using the ACC.

ACC Actions

To customize and refine the ACC display, you can add and delete tabs, add and delete widgets, set local and global filters, and interact with the widgets.

- Working with Tabs and Widgets
- Working with Filters—Local Filters and Global Filters

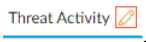
Working with Tabs and Widgets

The following options describe how to use and customize tabs and widgets.

- Add a custom tab.
  1. Select Add ( ) along the list of tabs.
  2. Add a **View Name**. This name will be used as the name for the tab. You can add up to 10 custom tabs.

- Edit a tab.

  Select the tab and click edit next to the tab name to edit the tab.

  Example: 

.

- Set a tab as default
  1. Edit a tab.
  2. Select to set the current tab as the default. Each time you log in to the firewall, this tab will display.

- Save a tab state
  1. Edit a tab.
  2. Select to save your preferences in the current tab as the default.

     The tab state including any filters that you may have set are synchronized across HA peers.

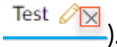
- Export a tab
  1. Edit a tab.
  2. Select to export the current tab. The tab downloads to your computer as a .txt file. You must enable pop-ups to download the file.

- Import a tab
  1. Add a custom tab.
  2. Select to import a tab.
  3. Browse to the text (.txt) file and select it.

- See which widgets are included in a view.
  1. Select the view and click edit ( ).
  2. Select the **Add Widgets** drop-down to review selected widgets.

- Add a widget or a widget group.
  1. Add a new tab or edit a predefined tab.
  2. Select **Add Widget** and then select the widget you want to add. You can select a maximum of 12 widgets.
  3. (Optional) To create a two-column layout, select **Add Widget Group**. You can drag and drop widgets into the two-column display. As you drag the widget into the layout, a placeholder will display for you to drop the widget.

     You cannot name a widget group.

- Delete a tab, widget, or widget group.
  - To delete a custom tab, select the tab and click delete (

).

    You cannot delete a predefined tab.
  - To delete a widget or widget group, edit the tab and then click delete ([X]). You cannot undo a deletion.

- Reset the default view.

  On a predefined view, such as the **Blocked Activity** view, you can delete one or more widgets. If you want to reset the layout to include the default set of widgets for the tab, edit the tab and **Reset View**.

Working with Filters—Local Filters and Global Filters

To hone the details and finely control what the ACC displays, you can use filters:

- **Local Filters**—Local filters are applied on a specific widget. A local filter allows you to interact with the graph and customize the display so that you can dig in to the details and access the information you want to monitor on a specific widget. You can apply a local filter in two ways: click into an attribute in the graph or table; or select **Set Filter** within a widget. **Set Filter** allows you to set a local filter that is persistent across reboots.
- **Global filters—**Global filters are applied across the ACC. A global filter allows you to pivot the display around the details you care most about and exclude the unrelated information from the current display. For example, to view all events related to a specific user and application, you can apply the user's IP address and specify the application to create a global filter that displays only information pertaining to that user and application through all the tabs and widgets on the ACC. Global filters are not persistent across logins.

  Global filters can be applied in three ways:

- **Set a global filter from a table**—Select an attribute from a table in any widget and apply the attribute as a global filter.
- **Add a widget filter to be a global filter**—Hover over the attribute and click the arrow icon to the right of the attribute. This option allows you to elevate a local filter used in a widget and apply the attribute globally to update the display across all tabs on the ACC.
- **Define a global filter**—Define a filter using the **Global Filters** pane on the ACC.

- Set a local filter.

You can also click an attribute in the table below the graph to apply it as a local filter.

1. Select a widget and click Filter ( ).
2. Add ( ) filters you want to apply.
3. Click **Apply**. These filters are persistent across reboots.

The number of local filters applied on a widget are indicated next to the widget name.

- Set a global filter from a table.

  Hover over an attribute in a table and click the arrow that appears to the right of the attribute.

- Set a global filter using the Global Filters pane.

  Add ( ) filters you want to apply.

- Promote a local filter to as global filter.
  1. On any table in a widget, select an attribute. This sets the attribute as a local filter.
  2. To promote the filter to a global filter, hover over the attribute and click the arrow to the right of the attribute.

- Remove a filter.

  Click Remove ( ) to remove a filter.
  - **Global filters**—Located in the Global Filters pane.
  - **Local filters**—Click Filter ( ) to bring up the Set Local Filters dialog and then select the filter and remove it.

- Clear all filters.
  - **Global filters**—**Clear all** Global Filters.
  - **Local filters**—Select a widget and click Filter ( ). Then **Clear all** in the Set Local Filters widget.

- Negate filters.

  Select an attribute and Negate ( ) a filter.
  - **Global filters**—Located in the Global Filters pane.
  - **Local filters**—Click Filter ( ) to bring up the Set Local Filters dialog add a filter, and then negate it.

- View what filters are in use.
  - **Global filters**—The number of global filters applied are displayed on the left pane under Global Filters.
  - **Local filters**—The number of local filters applied on a widget are displayed next to the widget name. To view the filters, click **Set Local Filters**.

Monitor

The following topics describe the firewall reports and logs you can use to monitor activity on your network:

- Monitor > Logs
- Monitor > External Logs
- Monitor > Automated Correlation Engine
- Monitor > Packet Capture
- Monitor > App Scope
- Monitor > Session Browser
- Monitor > Block IP List
- Monitor > Botnet
- Monitor > PDF Reports
- Monitor > Manage Custom Reports
- Monitor > Reports

Monitor > Logs

The following topics provide additional information about monitoring logs.

What do you want to know?	See:
Tell me about the different types of logs.	Log Types
Filter logs. Export logs. View details for individual log entries. Modify the log display.	Log Actions
Looking for more?	Monitor and manage logs.

Log Types

- **Monitor** > **Logs**

The firewall displays all logs so that role-based administration permissions are respected. Only the information that you are permitted to see is visible, which varies depending on the types of logs you are viewing. For information on administrator permissions, see Device > Admin Roles.

Log Type	Description
Traffic	Displays an entry for the start and end of each session. Each entry includes the date and time, source and destination zones, addresses and ports, application name, security rule name applied to the flow, rule action (**allow**, **deny**, or **drop**), ingress and egress interface, number of bytes, and session end reason. The Type column indicates whether the entry is for the start or end of the session, or whether the session was denied or dropped. A “drop” indicates that the security rule that blocked the traffic specified “any” application, while a “deny” indicates the rule identified a specific application. If traffic is dropped before the application is identified, such as when a rule drops all traffic for a specific service, the application is shown as “not-applicable”. Drill down in traffic logs for more details on individual entries, artifacts, and actions: • Click Details () to view additional details about the session, such as whether an ICMP entry aggregates multiple sessions between the same source and destination (the **Count** value will be greater than one). • On a firewall with an active AutoFocus™ license, hover next to an IP address, filename, URL, user agent, threat name, or hash

Log Type	Description
	contained in a log entry and click the drop-down () to open the AutoFocus Intelligence Summary for that artifact. • To add a device to the quarantine list (**Device** > **Device Quarantine**), open the **Host ID** drop-down for the device and **Block Device** (in the pop-up dialog).
Threat	Displays an entry for each security alarm generated by the firewall. Each entry includes the date and time, a threat name or URL, the source and destination zones, addresses, and ports, the application name, security rule name applied to the flow, and the alarm action (**allow** or **block**) and severity. The Type column indicates the type of threat, such as “virus” or “spyware;” the Name column is the threat description or URL; and the Category column is the threat category (such as “keylogger”) or URL category. Drill down in threat logs for more details on individual entries, artifacts, and actions: • Click Details () to view additional details about the threat, such as whether the entry aggregates multiple threats of the same type between the same source and destination (the **Count** value will be greater than one). • On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash contained in a log entry and click the drop-down () to open the AutoFocus Intelligence Summary for that artifact. • If local packet captures are enabled, click Download () to access captured packets. To enable local packet captures, refer to the subsections under **Objects** > **Security Profiles**. • To view more details about a threat or to quickly configure threat exemptions directly from the threat logs, click the threat name in the **Name** column. The Exempt Profiles list shows all custom Antivirus, Anti-spyware, and Vulnerability protection profiles. To configure an exemption for a threat signature, select the check box to the left of the security profile name and save your change. To add exemptions for IP Addresses (up to 100 IP addresses per signature), highlight the security profile, add the IP address(es) in the Exempt IP Addresses section and click **OK** to save. To view or modify the exemption, go to the associated security profile and click the **Exceptions** tab. For example, if the threat type is vulnerability, select **Objects** > **Security Profiles** > **Vulnerability Protection**, click the associated profile then click the **Exceptions** tab. • To add a device to the quarantine list (**Device** > **Device Quarantine**), open the **Host ID** drop-down for the device and **Block Device** (in the pop-up dialog).
URL Filtering	Displays logs for URL filters, which control access to websites and whether users can submit credentials to websites.

Log Type	Description
	Select Objects > Security Profiles > URL Filtering to define URL filtering settings, including which URL categories to block or allow and to which you want to grant or disable credential submissions. You can also enable logging of the HTTP header options for the URL. On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash contained in a log entry and click the drop-down ( ) to open the AutoFocus Intelligence Summary for that artifact.
WildFire Submissions	Displays logs for files and email links that the firewall forwarded for WildFire™ analysis. The WildFire cloud analyzes the sample and returns analysis results, which include the WildFire verdict assigned to the sample (benign, malware, grayware, or phishing). You can confirm if the firewall allowed or blocked a file based on Security policy rules by viewing the Action column. On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash (in the File Digest column) contained in a log entry and click the drop-down ( ) to open the AutoFocus Intelligence Summary for the artifact.
Data Filtering	Displays logs for the security policies with attached Data Filtering profiles, to help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall, and File Blocking profiles, that prevent certain file types from being uploaded or downloaded. To configure password protection for access the details for a log entry, click ↓. Enter the password and click **OK**. Refer to Device > Response Pages for instructions on changing or deleting the data protection password. *The system prompts you to enter the password only once per session.*
HIP Match	Displays all HIP matches that the GlobalProtect™ gateway identifies when comparing the raw HIP data reported by the agent to the defined HIP objects and HIP profiles. Unlike other logs, a HIP match is logged even when it does not match a security policy. For more information, refer to Network > GlobalProtect > Portals. To add a device to the quarantine list (**Device** > **Device Quarantine**), open the **Host ID** drop-down for the device and **Block Device** (in the pop-up dialog).
GlobalProtect	Displays GlobalProtect connection logs. Use this information to identify your GlobalProtect users and their client OS version, troubleshoot connection and performance issues, and identify the portal and gateways to which users connect.

Log Type	Description
	To add a device to the quarantine list (**Device** > **Device Quarantine**), open the **Host ID** drop-down for the device and **Block Device** (in the pop-up dialog).
IP-Tag	Displays information about how and when a tag was applied to a particular IP address. Use this information to determine when and why a particular IP address was placed in an address group and what policy rules impact that address. The log includes Receive Time (the date and time when the first and last packet of the session arrived), Virtual System, Source IP-Address, Tag, Event, Timeout, Source Name, and Source Type.
User-ID™	Displays information about IP address-to-username mappings, such as the source of the mapping information, when the User-ID agent performed the mapping, and the remaining time before mappings expire. You can use this information to help troubleshoot User-ID issues. For example, if the firewall is applying the wrong policy rule for a user, you can view the logs to verify whether that user is mapped to the correct IP address and whether the group associations are correct.
Decryption	Displays information about decryption sessions and undecrypted sessions for traffic that a No Decryption profile controls, including GlobalProtect sessions. By default, the logs show information about unsuccessful SSL Decryption handshakes. You can enable logging for successful SSL Decryption handshakes in Decryption Policy rules **Options**. Logs display a wealth of information that enables you to identify weak protocols and cipher suites (key exchange, encryption, and authentication algorithms), bypassed decryption activity, decryption failures and their causes (e.g., incomplete certificate chain, client authentication, pinned certificates), session end reasons, and more. For example, use the information to determine whether you want to allow sites that use weak protocols and algorithms. It may be better to block weak sites that you don't need to access for business purposes. For traffic the firewall doesn't decrypt and to which you apply a No Decryption profile, the log shows sessions blocked because of server certificate verification issues. The default Decryption Log size is 32 MB. However, if you decrypt a lot of traffic or if you enable logging successful SSL Decryption handshakes, you will probably need to increase the log size (**Device** > **Setup** > **Management** > **Logging and Reporting Settings** and edit the **Log Storage** quotas). If you don't have unallocated log space, consider tradeoffs between Decryption Log size and other log sizes. The more you log, the more resources the logs consume.
GTP	Displays event-based logs that include information on the wide range of GTP attributes. These include GTP event type, GTP event message type, APN, IMSI, IMEI, End User IP address, in addition to

Log Type	Description
	the TCP/IP information that the next-generation firewall identifies such as application, source and destination address and timestamp.
Tunnel Inspection	Displays an entry for the start and end of each inspected tunnel session. The log includes the Receive Time (date and time the first and last packet in the session arrived), Tunnel ID, Monitor Tag, Session ID, Security rule applied to the tunnel traffic, and more. See Policies > Tunnel Inspection for more information.
SCTP	Displays SCTP events and associations based on logs generated by the firewall while it performs stateful inspection, protocol validation, and filtering of SCTP traffic. SCTP logs include information on the wide range of SCTP and its payload protocol attributes, such as SCTP event type, chunk type, SCTP cause code, Diameter Application ID, Diameter Command Code, and chunks. This SCTP information is provided in addition to the general information that the firewall identifies, such as source and destination address, source and destination port, rule, and timestamp. See Objects > Security Profiles > SCTP Protection for more information.
Configuration	Displays an entry for each configuration change. Each entry includes the date and time, the administrator username, the IP address from where the change was made, the type of client (web interface or CLI), the type of command executed, whether the command succeeded or failed, the configuration path, and the values before and after the change.
System	Displays an entry for each system event. Each entry includes the date and time, the event severity, and an event description.
Alarms	The alarms log records detailed information on alarms that are generated by the system. The information in this log is also reported in Alarms. Refer to Define Alarm Settings.
Authentication	Displays information about authentication events that occur when end users try to access network resources for which access is controlled by Authentication policy rules. You can use this information to help troubleshoot access issues and to adjust your Authentication policy as needed. In conjunction with correlation objects, you can also use Authentication logs to identify suspicious activity on your network, such as brute force attacks. Optionally, you can configure Authentication rules to Log Authentication Timeouts. These timeouts relate to the period of time when a user need authenticate for a resource only once but can access it repeatedly. Seeing information about the timeouts helps you decide if and how to adjust them. *System logs record authentication events relating to GlobalProtect and to administrator access to the web interface.*

Log Type	Description
Unified	Displays the latest Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering log entries in a single view. The collective log view enables you to investigate and filter these different types of logs together (instead of searching each log set separately). Or, you can choose which log types to display: click the arrow to the left of the filter field and select **traffic**, **threat**, **url**, **data**, and/or **wildfire** to display only the selected log types. On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash contained in a log entry and click the drop-down ( ) to open the AutoFocus Intelligence Summary for that artifact. The firewall displays all logs so that role-based administration permissions are respected. When viewing Unified logs, only the logs that you have permission to see are displayed. For example, an administrator who does not have permission to view WildFire Submissions logs will not see WildFire Submissions log entries when viewing Unified logs. For information on administrator permissions, refer to Device > Admin Roles. *You can use the Unified log set with the AutoFocus threat intelligence portal. Set up an AutoFocus search to add AutoFocus search filters directly to the Unified log filter field.* To add a device to the quarantine list (**Device** > **Device Quarantine**), open the **Host ID** drop-down for the device and **Block Device** (in the pop-up dialog).

Log Actions

The following table describes log actions.

Action	Description
Filter Logs	Each log page has a filter field at the top of the page. You can add artifacts to the field, such as an IP address or a time range, to find matching log entries. The icons to the right of the field enable you to apply, clear, create, save, and load filters.  • Create a filter: • Click an artifact in a log entry to add that artifact to the filter. • Click **Add** ( ) to define new search criteria. For each criterion, select the **Connector** that defines the search type (**and** or **or**), the **Attribute** on which to base the search, an **Operator** to define the scope of the search, and a **Value** for evaluation against log entries. **Add** each criterion to the filter field and **Close** when you finish. You can then apply ( ) the filter.

Action	Description
	If the Value string matches an Operator (such as has or in), enclose the string in quotation marks to avoid a syntax error. For example, if you filter by destination country and use ***IN*** *as a Value to specify INDIA, enter the filter as* ***(dstloc eq "IN")****.* *The log filter* ***(receive_time in last-60-seconds)*** *causes the number of log entries (and log pages) displayed to grow or shrink over time.* • Apply filters—Click Apply Filter ( ) to display log entries that match the current filter. • Delete filters—Click Clear Filter ( ) to clear the filter field. • Save a filter—Click Save Filter ( ), enter a name for the filter, and click **OK**. • Use a saved filter—Click Load Filter ( ) to add a saved filter to the filter field.
Export Logs	Click Export to CSV ( ) to export all logs matched to the current filter to a CSV-formatted report and continue to **Download file**. By default, the report contains up to 2,000 lines of logs. To change the line limit for generated CSV reports, select **Device** > **Setup** > **Management** > **Logging and Reporting Settings** > **Log Export and Reporting** and enter a new **Max Rows in CSV Export** value.
Highlight Policy Actions	Select to highlight log entries that match the action. The filtered logs are highlighted in the following colors: • Green—Allow • Yellow—Continue, or override • Red—Deny, drop, drop-icmp, rst-client, reset-server, reset-both, block-continue, block-override, block-url, drop-all, sinkhole
Change Log Display	To customize the log display: • Change the automatic refresh interval—Select an interval from the interval drop-down (**60 seconds**, **30 seconds**, **10 seconds**, or **Manual**). • Change the number and order of entries displayed per page—Log entries are retrieved in blocks of 10 pages. • Use the paging controls at the bottom of the page to navigate through the log list. • To change the number of log entries per page, select the number of rows from the per page drop-down (**20**, **30**, **40**, **50**, **75**, or **100**). • To sort the results in ascending or descending order, use the **ASC** or **DESC** drop-down. • Resolve IP addresses to domain names—Select **Resolve Hostname** to begin resolving external IP addresses to domain names. • Change the order in which logs are displayed—Select **DESC** to display logs in descending order beginning with log entries with the most recent Receive Time. Select **ASC** to display logs in ascending order beginning with log entries with the oldest Receive Time.

Action	Description
View Details for Individual Log Entries	To view information about individual log entries: • To display additional details, click Details ( ) for an entry. If the source or destination has an IP address to domain or username mapping defined in the **Addresses** page, the name is presented instead of the IP address. To view the associated IP address, move your cursor over the name. • On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash contained in a log entry and click the drop-down ( ) to open the AutoFocus Intelligence Summary for the artifact.

Monitor > External Logs

Use this page to view logs ingested from the Traps™ Endpoint Security Manager (ESM) into Log Collectors that are managed by Panorama™. To view Traps ESM logs on Panorama, do the following:

- On the Traps ESM server, configure Panorama as a Syslog server and select the logging events to forward to Panorama. The events can include security events, policy changes, agent and ESM Server status changes, and changes to configuration settings.
- On a Panorama that is deployed in Panorama mode with one or more Managed Log Collectors, set up a log ingestion profile (Panorama > Log Ingestion Profile) and attach the profile to a Collector Group (Panorama > Collector Groups) in which to store the Traps ESM logs.

External logs are not associated with a device group and are visible only when you select **Device Group**: **All** because the logs are not forwarded from firewalls.

Log Type	Description
Monitor > **External Logs** > **Traps ESM** > **Threat**	These threat events include all prevention, notification, provisional, and post-detection events that are reported by the Traps agents.
Monitor > **External Logs** > **Traps ESM** > **System**	ESM Server system events include changes related to ESM status, licenses, ESM Tech Support files, and communication with WildFire.
Monitor > **External Logs** > **Traps ESM** > **Policy**	Policy change events include changes to rules, protection levels, content updates, hash control logs, and verdicts.
Monitor > **External Logs** > **Traps ESM** > **Agent**	Agent change events occur on the endpoint and include changes to content updates, licenses, software, connection status, one-time action rules, processes and services, and quarantined files.
Monitor > **External Logs** > **Traps ESM** > **Config**	ESM configuration change events include system-wide changes to licensing, administrative users and roles, processes, restriction settings, and conditions.

Panorama can correlate discrete security events on the endpoints with events on the network to trace any suspicious or malicious activity between the endpoints and the firewall. To view correlated events that Panorama identifies, see Monitor > Automated Correlation Engine > Correlated Events.

Monitor > Automated Correlation Engine

The automated correlation engine tracks patterns on your network and correlates events that indicate an escalation in suspicious behavior or events that amount to malicious activity. The engine functions as your personal security analyst who scrutinizes isolated events across the different sets of logs on the firewall, queries the data for specific patterns, and connects the dots so that you have actionable information.

The correlation engine uses correlation objects that generate correlated events. Correlated events collate evidence to help you trace commonality across seemingly unrelated network events and provide the focus for incident response.

The following models support the automated correlation engine:

- Panorama—M-Series appliances and virtual appliances
- PA-3200 Series firewalls
- PA-5200 Series firewalls
- PA-7000 Series firewalls

What do you want to know?	See:
What are correlation objects?	Monitor > Automated Correlation Engine > Correlation Objects
What is a correlated event? Where do I see the match evidence for a correlation match?	Monitor > Automated Correlation Engine > Correlated Events
How can I see a graphical view of correlation matches?	See the Compromised Hosts widget in ACC.
Looking for more?	Use the Automated Correlation Engine

Monitor > Automated Correlation Engine > Correlation Objects

To counter the advances in exploits and malware distribution methods, correlation objects extend the signature-based malware detection capabilities on the firewall. They provide the intelligence for identifying suspicious behavior patterns across different sets of logs and they gather the evidence required to investigate and promptly respond to an event.

A correlation object is a definition file that specifies patterns for matching, the data sources to use for performing the lookups, and the time period within which to look for these patterns. A pattern is a boolean structure of conditions that query the data sources, and each pattern is assigned a severity and a threshold, which is number of time the pattern match occurs within a defined time limit. When a pattern match occurs, a correlation event is logged.

The data sources used for performing lookups can include the following logs: application statistics, traffic, traffic summary, threat summary, threat, data filtering, and URL filtering. For example, the definition for a correlation object can include a set of patterns that query the logs for evidence of infected hosts, evidence of malware patterns, or for lateral movement of malware in the traffic, url filtering, and threat logs.

Correlation objects are defined by Palo Alto Networks® and are packaged with content updates. You must have a valid threat prevention license to get content updates.

By default, all correlation objects are enabled. To disable an object, select the object and **Disable** it.

Correlation Object Fields	Description
Name and Title	The label indicates the type of activity that the correlation object detects.
ID	A unique number identifies the correlation object. This number is in the 6000 series.
Category	A summary of the kind of threat or harm posed to the network, user, or host.
State	The state indicates whether the correlation object is enabled (active) or disabled (inactive).
Description	The description specifies the match conditions for which the firewall or Panorama will analyze logs. It describes the escalation pattern or progression path that will be used to identify malicious activity or suspicious host behavior.

Monitor > Automated Correlation Engine > Correlated Events

Correlated events expand the threat detection capabilities on the firewall and Panorama; the correlated events gather evidence of suspicious or unusual behavior of users or hosts on the network.

The correlation object makes it possible to pivot on certain conditions or behaviors and trace commonalities across multiple log sources. When the set of conditions specified in a correlation object are observed on the network, each match is logged as a correlated event.

The correlated event includes the details listed in the following table.

Field	Description
Match Time	The time the correlation object triggered a match.
Update Time	The timestamp when the match was last updated.
Object Name	The name of the correlation object that triggered the match.
Source Address	The IP address of the user from whom the traffic originated
Source User	The user and user group information from the directory server, if User-ID™ is enabled.
Severity	A rating that classifies the risk based on the extent of damage caused.
Summary	A description that summarizes the evidence gathered on the correlated event.
Host ID	The Host ID of the device. To add a device to the quarantine list (**Device** > **Device Quarantine**), click the down arrow next to the device's **Host ID** and select **Block Device** in the pop-up window that displays.

To view the detailed log view, click Details ( ) for an entry. The detailed log view includes all the evidence for a match:

Tab	Description
Match Information	**Object Details**—Presents information on the correlation object that triggered the match. For information on correlation objects, see Monitor > Automated Correlation Engine > Correlation Objects.
	Match Details—A summary of the match details that includes the match time, last update time on the match evidence, severity of the event, and an event summary.
Match Evidence	This tab includes all the evidence that corroborates the correlated event. It lists detailed information on the evidence collected for each session.

See a graphical display of the information in the **Correlated Events** tab, see the Compromised Hosts widget on the **ACC** > **Threat Activity** tab. In the Compromised Hosts widget, the display is aggregated by source user and IP address and sorted by severity.

To configure notifications when a correlated event is logged, go to the **Device** > **Log Settings** or **Panorama** > **Log Settings** tab.

Monitor > Packet Capture

All Palo Alto Networks firewalls have a built-in packet capture (pcap) feature you can use to capture packets that traverse the network interfaces on the firewall. You can then use the captured data for troubleshooting purposes or to create custom application signatures.

The packet capture feature is CPU-intensive and can degrade firewall performance. Only use this feature when necessary and make sure to turn it off after you collect the required packets.

What do you want to know?	See:
What are the different methods the firewall can use to capture packets?	Packet Capture Overview
How do I generate a custom packet capture?	Building Blocks for a Custom Packet Capture
How do I generate packet captures when the firewall detects a threat?	Enable Threat Packet Capture
Where do I download a packet capture?	Packet Capture Overview
Looking for more?	
• Turn on extended packet capture for security profiles.	Device > Setup > Content-ID
• Use packet capture to write custom application signatures.	See Custom Signatures.
• Prevent a firewall admin from viewing packet captures.	Define Web Interface Administrator Access.
• See an example.	See Take Packet Captures.

Packet Capture Overview

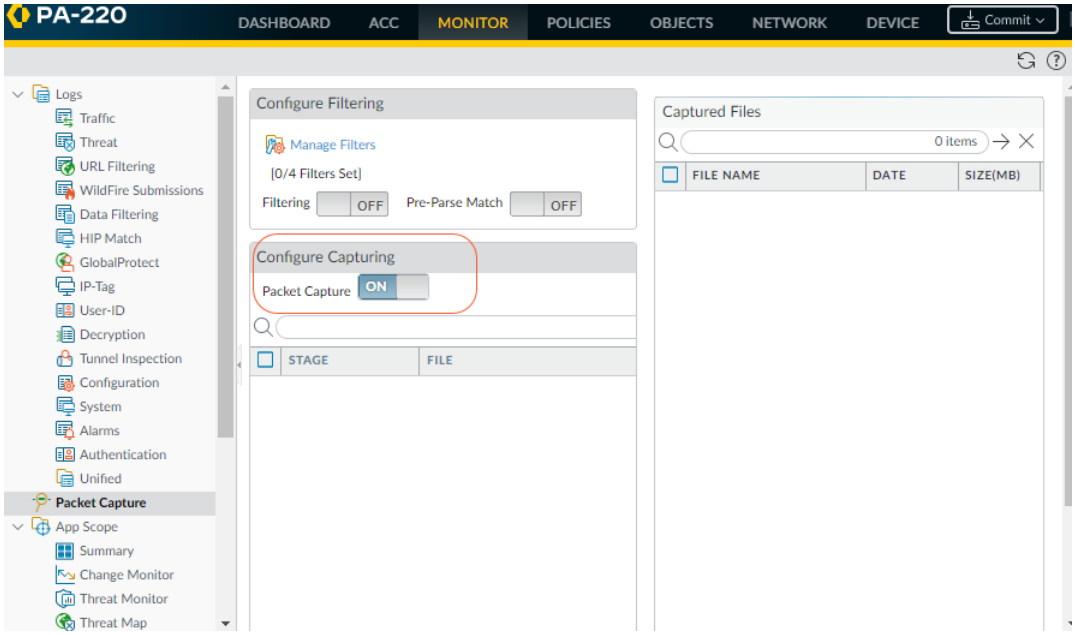
You can configure a Palo Alto Networks firewall to perform a custom packet capture or a threat packet capture.

- **Custom Packet Capture**—Capture packets for all traffic or traffic based on filters you define. For example, you can configure the firewall to capture only packets to and from a specific source and destination IP address or port. Use these packet captures to troubleshoot network traffic-related issues or to gather application attributes to write custom application signatures (**Monitor** > **Packet Capture**). You define the file name based on the stage (Drop, Firewall, Receive, or Transmit) and, after the PCAP is complete, you download the PCAP in the Captured Files section.

- **Threat Packet Capture**—Capture packets when the firewall detects a virus, spyware, or vulnerability. You enable this feature in Antivirus, Anti-Spyware, and Vulnerability Protection security profiles. These packet captures provide context around a threat to help you determine if an attack is successful or to learn more about the methods used by an attacker. The action for the threat must be set to either allow or alert; otherwise, the threat is blocked and packets cannot be captured. You configure this type of packet capture in the **Objects** > **Security Profiles**. To download (↓) pcaps, select **Monitor** > **Threat**.

Building Blocks for a Custom Packet Capture

The following table describes the components of the **Monitor** > **Packet Capture** page that you use to configure packet captures, enable packet capture, and to download packet capture files.



Custom Packet Capture Building Blocks	Configured In	Description
Manage Filters	Configure Filtering	When enabling custom packet captures, you should define filters so that only the packets that match the filters are captured. This will make it easier to locate the information you need in the pcaps and will reduce the processing power required by the firewall to perform the packet capture. Click **Add** to add a new filter and configure the following fields: • **Id**—Enter or select an identifier for the filter. • **Ingress Interface**—Select the ingress interface on which you want to capture traffic. • **Source**—Specify the source IP address of the traffic to capture. • **Destination**—Specify the destination IP address of the traffic to capture.

Custom Packet Capture Building Blocks	Configured In	Description
		• **Src Port**—Specify the source port of the traffic to capture. • **Dest Port**—Specify the destination port of the traffic to capture. • **Proto**—Specify the protocol number to filter (1-255). For example, ICMP is protocol number 1. • **Non-IP**—Choose how to treat non-IP traffic (exclude all IP traffic, include all IP traffic, include only IP traffic, or do not include an IP filter). Broadcast and AppleTalk are examples of Non-IP traffic. • **IPv6**—Select this option to include IPv6 packets in the filter.
Filtering	Configure Filtering	After defining filters, set the **Filtering** to **ON**. If filtering is **OFF**, then all traffic is captured.
Pre-Parse Match	Configure Filtering	This option is for advanced troubleshooting purposes. After a packet enters the ingress port, it proceeds through several processing steps before it is parsed for matches against pre#configured filters. It is possible for a packet, due to a failure, to not reach the filtering stage. This can occur, for example, if a route lookup fails. Set the **Pre-Parse Match** setting to **ON** to emulate a positive match for every packet entering the system. This allows the firewall to capture packets that do not reach the filtering process. If a packet is able to reach the filtering stage, it is then processed according to the filter configuration and discarded if it fails to meet filtering criteria.
Packet Capture	Configure Capturing	Click the toggle switch to turn packet capture **ON** or **OFF**. You must select at least one capture stage. Click **Add** and specify the following: • **Stage**—Indicate the point at which to capture packets: • **drop**—When packet processing encounters an error and the packet is dropped. • **firewall**—When the packet has a session match or a first packet with a session is successfully created. • **receive**—When the packet is received on the dataplane processor. • **transmit**—When the packet is transmitted on the dataplane processor.

Custom Packet Capture Building Blocks	Configured In	Description
		• **File**—Specify the capture file name. The file name should begin with a letter and can include letters, digits, periods, underscores, or hyphens. • **Packet Count**—Specify the maximum number of packets, after which capturing stops. • **Byte Count**—Specify the maximum number of bytes, after which capturing stops.
Captured Files	Captured Files	Contains a list of custom packet captures previously generated by the firewall. Click a file to download it to your computer. To delete a packet capture, select the packet capture and then **Delete** it. • **File Name**—Lists the packet capture files. The file names are based on the file name you specify for the capture stage • **Date**—Date the file was generated. • **Size (MB)**—The size of the capture file. After you turn on packet capture and then turn it off, you must click Refresh ( ) before any new PCAP files display in this list.
Clear All Settings	Settings	Click **Clear All Settings** to turn off packet capture and to clear all packet capture settings. *This does not turn off packet capture set in a security profile. For information on enabling packet capture on a security profile, see* Enable Threat Packet Capture.

Enable Threat Packet Capture

- Objects > Security Profiles

To enable the firewall to capture packets when it detects a threat, enable the packet capture option in the security profile.

First select **Objects** > **Security Profiles** and then modify the desired profile as described in the following table:

Packet Capture Options in Security Profiles	Location
Antivirus	Select a custom antivirus profile and, in the **Antivirus** tab, select **Packet Capture**.

Packet Capture Options in Security Profiles	Location
Anti-Spyware	Select a custom Anti-Spyware profile, click the **DNS Signatures** tab and, in the **Packet Capture** drop-down, select **single-packet** or **extended-capture**.
Vulnerability Protection	Select a custom Vulnerability Protection profile and, in the **Rules** tab, click **Add** to add a new rule or select an existing rule. Then select the **Packet Capture** drop-down and select **single-packet** or **extended-capture**.

In Anti-Spyware and Vulnerability Protection profiles, you can also enable packet capture on exceptions. Click the Exceptions tab and in the Packet Capture column for a signature, click the drop-down and select single-packet or extended-capture.

(Optional) To define the length of a threat packet capture based on the number of packets captured (which is based on a global setting), select **Device** > **Setup** > **Content-ID** and, in the Content-ID™ Settings section, modify the **Extended Packet Capture Length (packets)** field (range is 1-50; default is 5).

After you enable packet capture on a security profile, you need to verify that the profile is part of a security rule. For information on how to add a security profile to a security rule, see Security Policy Overview.

Each time the firewall detects a threat when packet capture is enabled on the security profile, you can download ( ) or export the packet capture.

Monitor > App Scope

The following topics describe App Scope features.

App Scope Overview

The App Scope reports provide graphical visibility into the following aspects of your network:

- Changes in application usage and user activity
- Users and applications that take up most of the network bandwidth
- Network threats

With the App Scope reports, you can quickly see if any behavior is unusual or unexpected, and helps pinpoint problematic behavior; each report provides a dynamic, user-customizable window into the network. The reports include options to select the data and ranges to display. On Panorama, you can also select the **Data Source** for the information that is displayed. The default data source (on new Panorama installations) uses the local database on Panorama, which stores logs forwarded by the managed firewalls; on an upgrade, the default data source is the **Remote Device Data** (managed firewall data). To fetch and display an aggregated view of the data directly from the managed firewalls, you now have to switch the source from **Panorama** to **Remote Device Data**.

Hovering the mouse over and clicking either the lines or bars on the charts switches to the ACC and provides detailed information about the specific application, application category, user, or source.

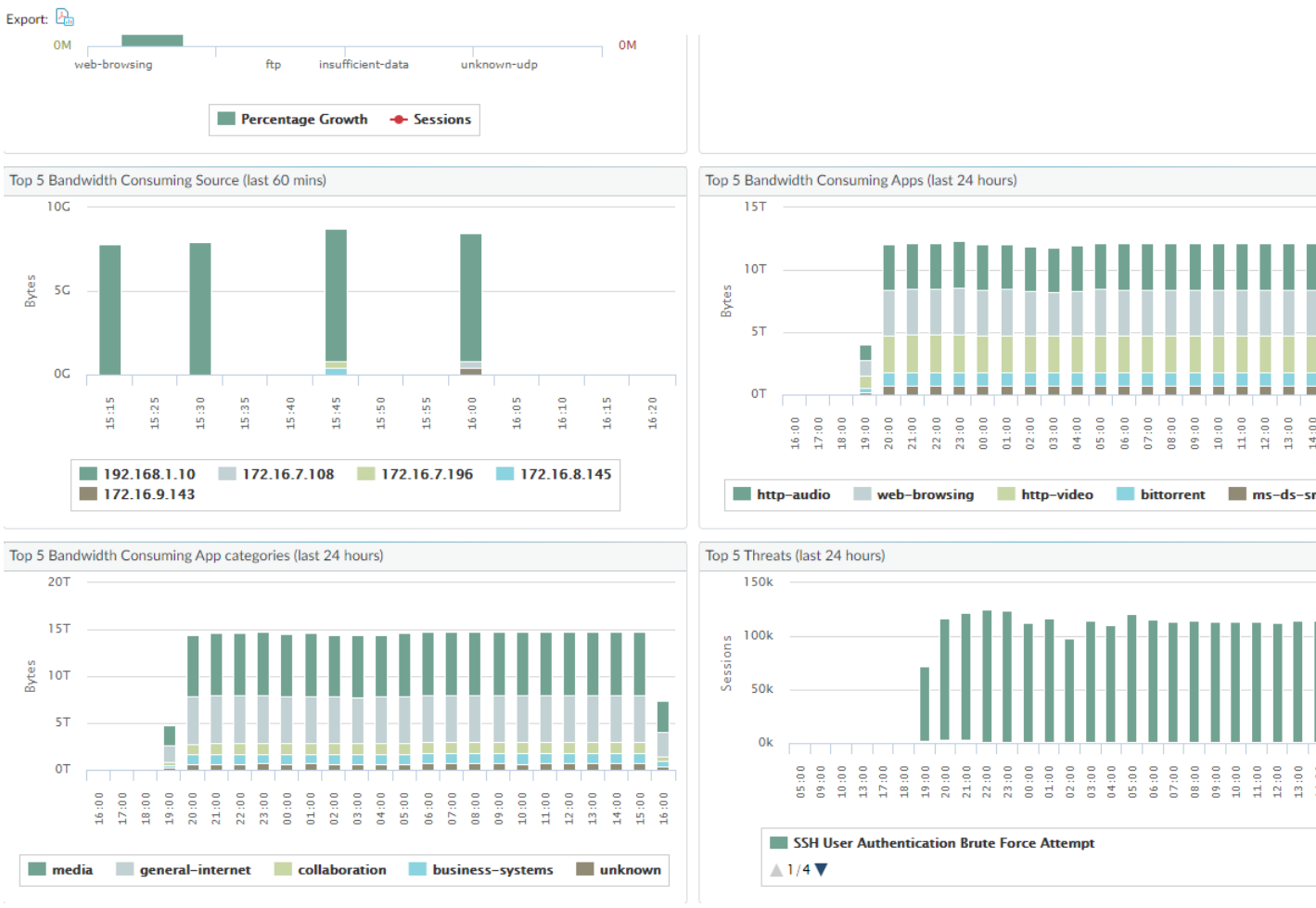
Application Command Center Charts	Description
Summary	App Scope Summary Report
Change Monitor	App Scope Change Monitor Report
Threat Monitor	App Scope Threat Monitor Report
Threat Map	App Scope Threat Map Report
Network Monitor	App Scope Network Monitor Report
Traffic Map	App Scope Traffic Map Report

App Scope Summary Report

The Summary report displays charts for the top five gainers, losers, and bandwidth consuming applications, application categories, users, and sources.

To export the charts in the summary report as a PDF, click **Export** ( ). Each chart is saved as a page in the PDF output.

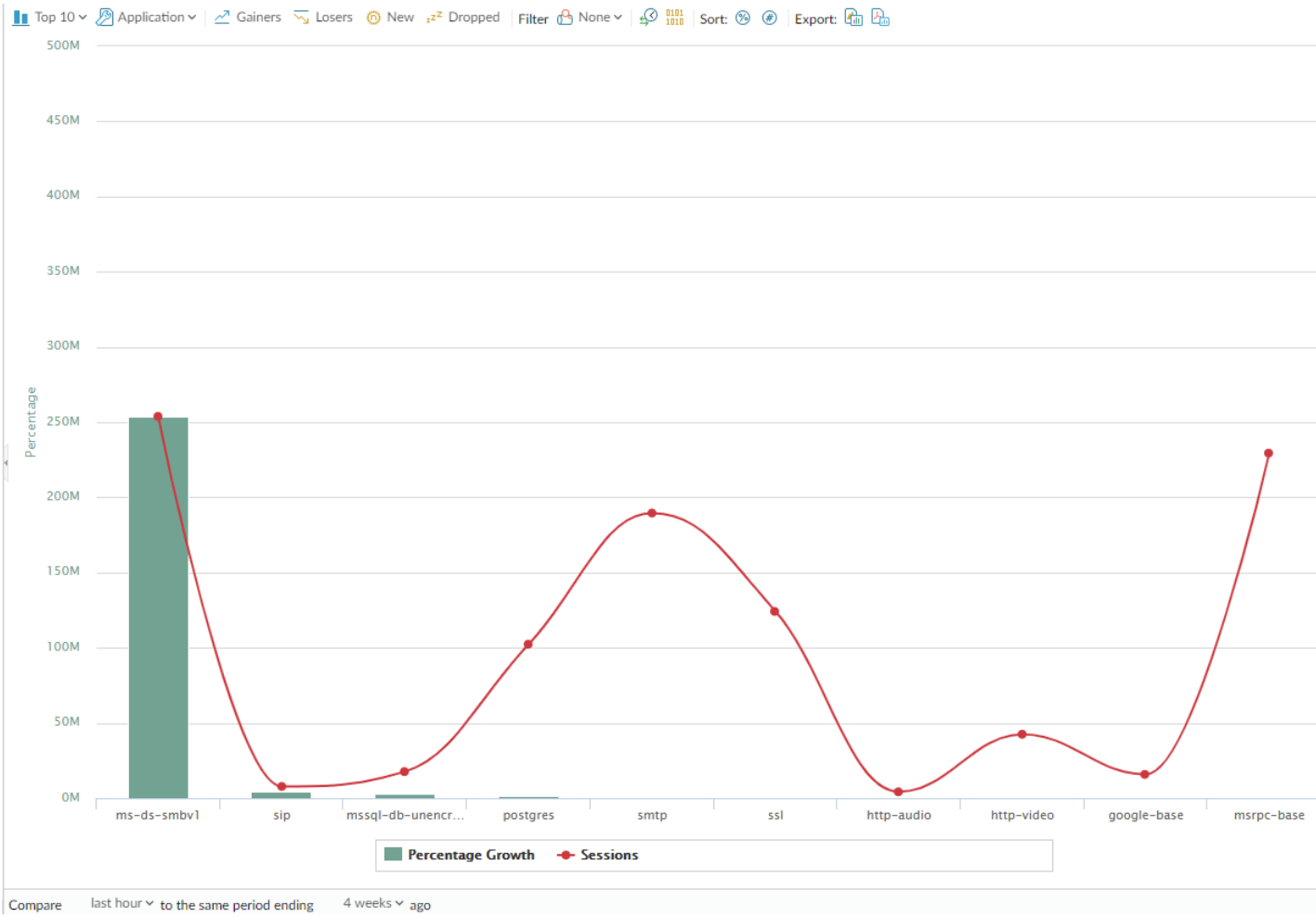
App Scope Summary Report



App Scope Change Monitor Report

The Change Monitor report displays changes over a specified time period. For example, the figure below displays the top applications that gained in use over the last hour as compared with the last 24-hour period. The top applications are determined by session count and sorted by percentage.

App Scope Change Monitor Report



This report contains the following options.

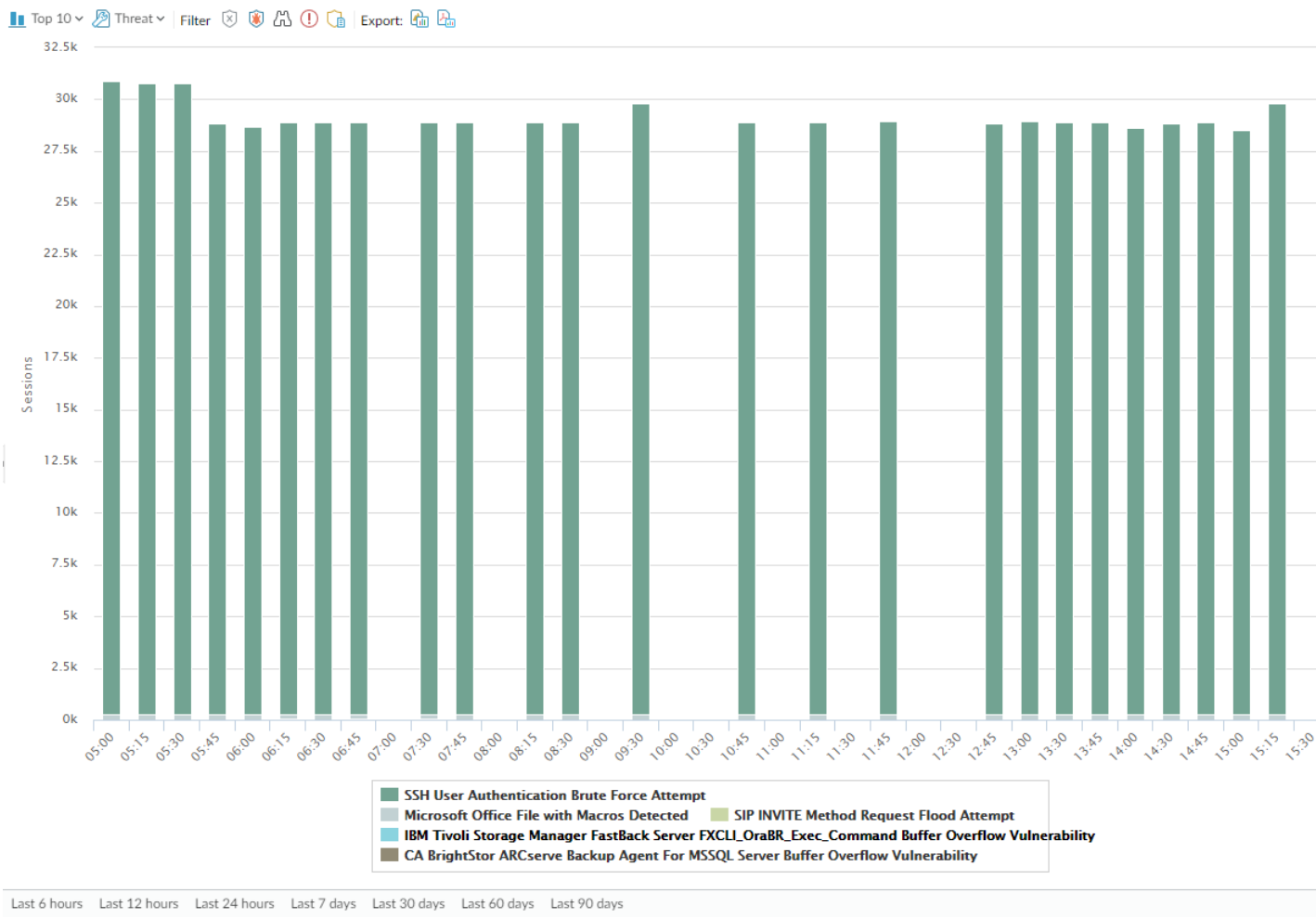
Change Monitor Report Options	Description
Top Bar	
Top 10	Determines the number of records with the highest measurement included in the chart.
Application	Determines the type of item reported: Application, Application Category, Source, or Destination.
Gainers	Displays measurements of items that have increased over the measured period.
Losers	Displays measurements of items that have decreased over the measured period.
New	Displays measurements of items that were added over the measure period.

Change Monitor Report Options	Description
Dropped	Displays measurements of items that were discontinued over the measure period.
Filter	Applies a filter to display only the selected item. None displays all entries.
Count Sessions and Count Bytes	Determines whether to display session or byte information.
Sort	Determines whether to sort entries by percentage or raw growth.
Export	Exports the graph as a .png image or as a PDF.
Bottom Bar	
Compare (interval)	Specifies the period over which the change measurements are taken.

App Scope Threat Monitor Report

The Threat Monitor report displays a count of the top threats over the selected time period. For example, the figure below shows the top 10 threat types for the past 6 hours.

App Scope Threat Monitor Report



Each threat type is color-coded as indicated in the legend below the chart. This report contains the following options.

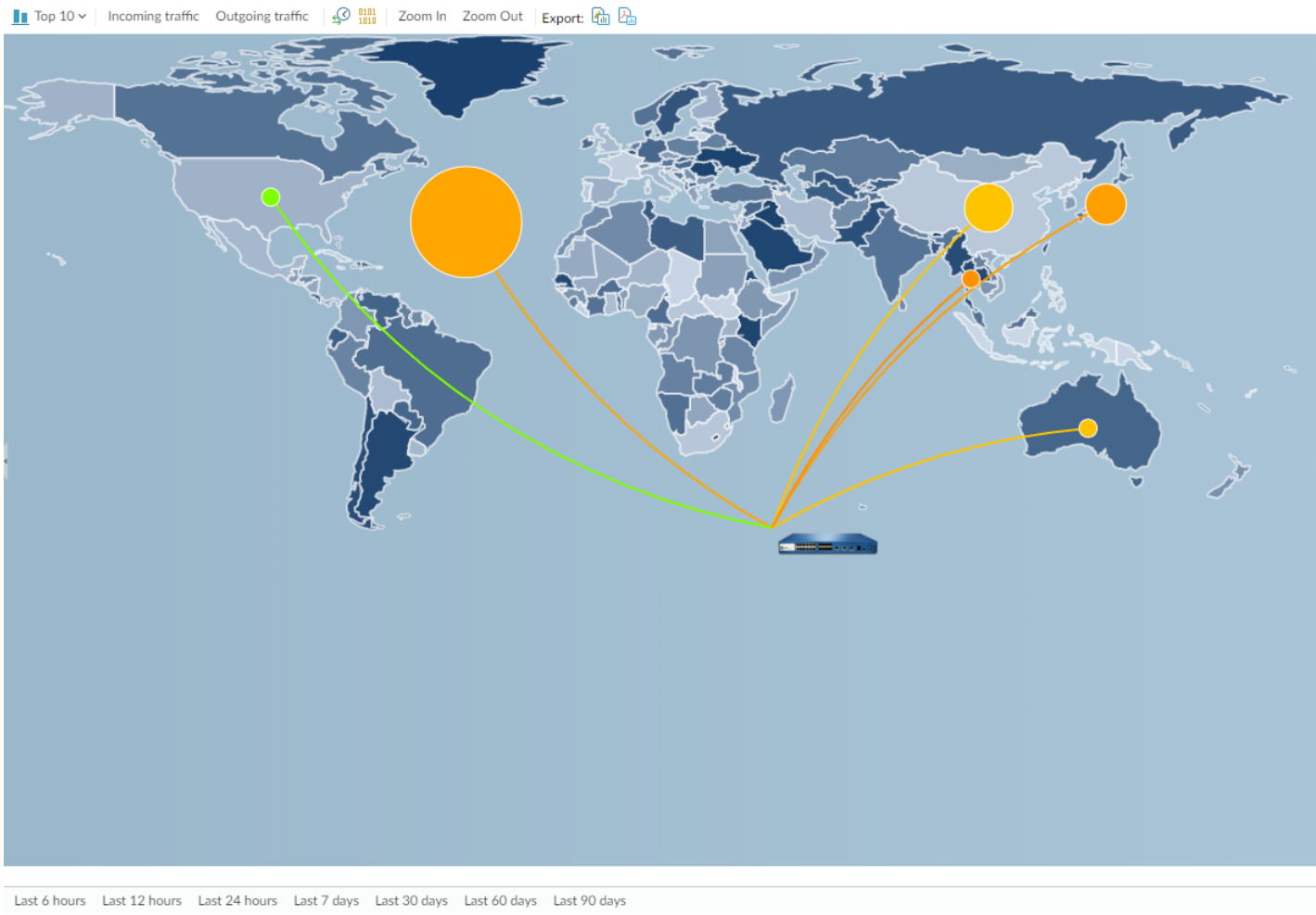
Threat Monitor Report Options	Description
Top Bar	
Top 10	Determines the number of records with the highest measurement included in the chart.
Threat	Determines the type of item measured: Threat, Threat Category, Source, or Destination.
Filter	Applies a filter to display only the selected item.
	Determines whether the information is presented in a stacked column chart or a stacked area chart.
Export	Exports the graph as a .png image or as a PDF.
Bottom Bar	

Threat Monitor Report Options	Description
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	Specifies the period over which the measurements are taken.

App Scope Threat Map Report

The Threat Map report shows a geographical view of threats, including severity.

App Scope Threat Map Report



Each threat type is color-coded as indicated in the legend below the chart. Click a country on the map to **Zoom In** and then **Zoom Out** as needed. This report contains the following options.

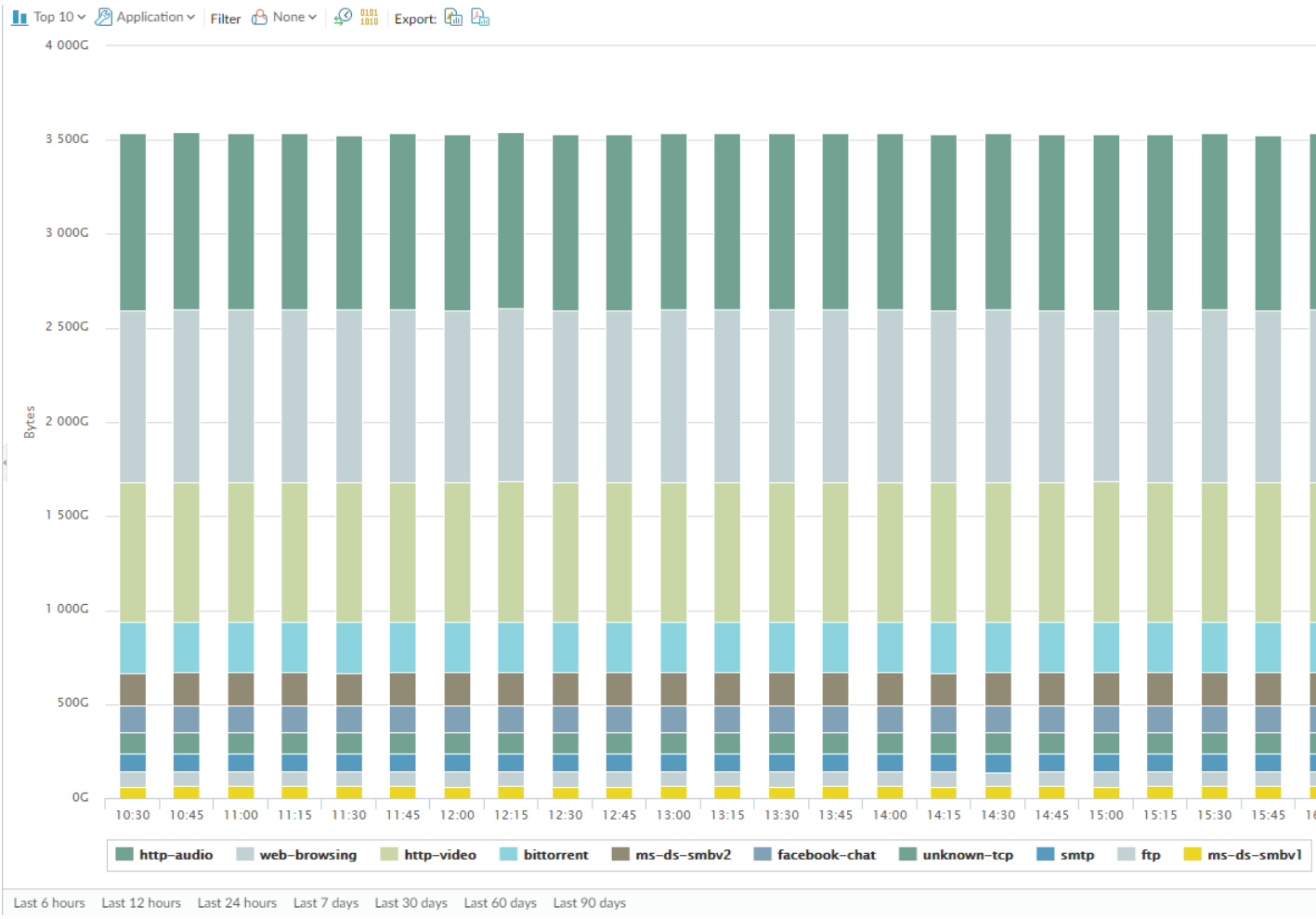
Threat Map Report Options	Description
Top Bar	
Top 10	Determines the number of records with the highest measurement included in the chart.
Incoming threats	Displays incoming threats.

Threat Map Report Options	Description
Outgoing threats	Displays outgoing threats.
Filter	Applies a filter to display only the selected item.
Zoom In and Zoom Out	Zoom in and zoom out of the map.
Export	Exports the graph as a .png image or as a PDF.
Bottom Bar	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	Indicates the period over which the measurements are taken.

App Scope Network Monitor Report

The Network Monitor report displays the bandwidth dedicated to different network functions over the specified period of time. Each network function is color-coded as indicated in the legend below the chart. For example, the image below shows application bandwidth for the past 7 days based on session information.

App Scope Network Monitor Report



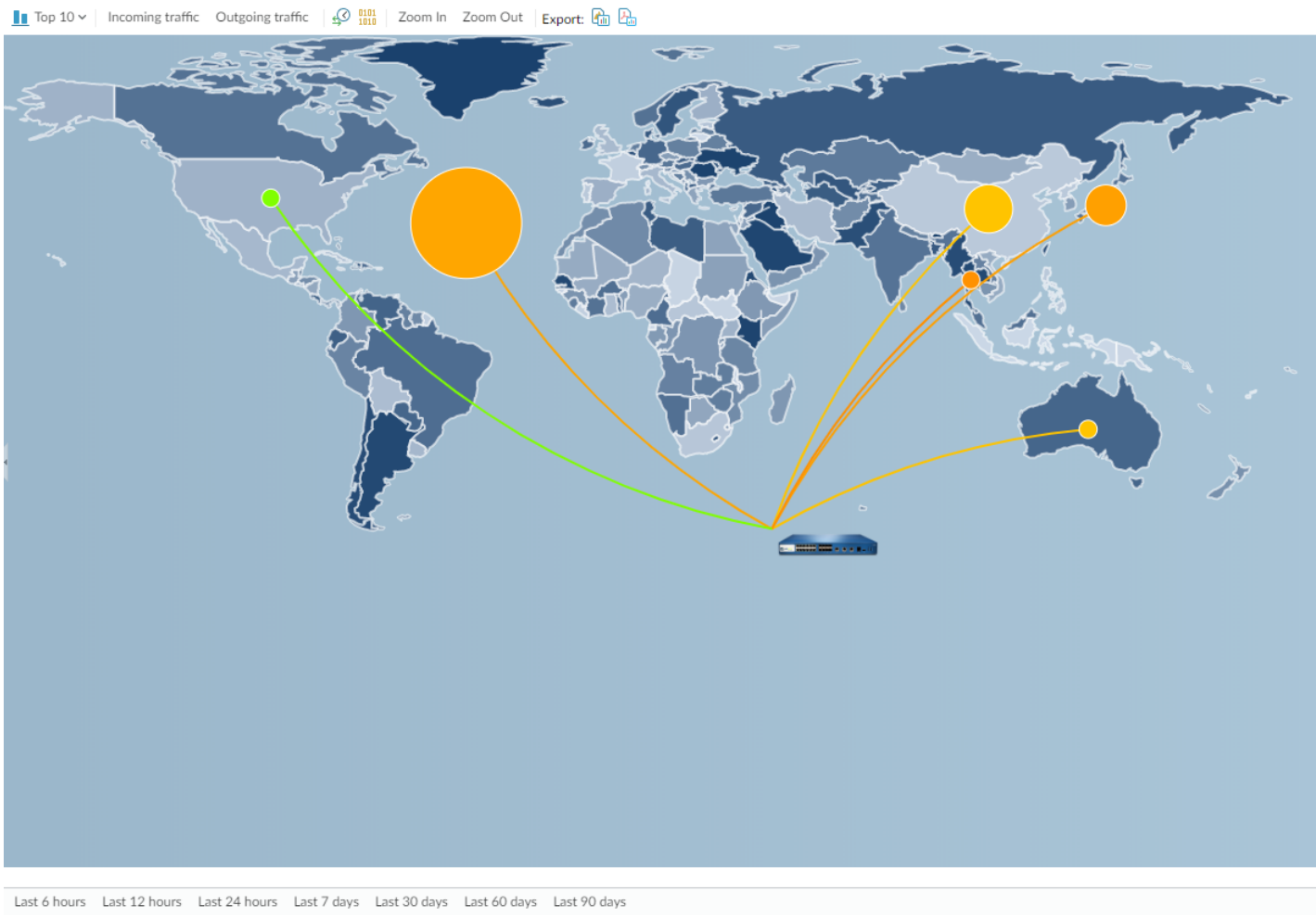
The report contains the following options.

Network Monitor Report Options	Description
Top Bar	
Top 10	Determines the number of records with the highest measurement included in the chart.
Application	Determines the type of item reported: Application, Application Category, Source, or Destination.
Filter	Applies a filter to display only the selected item. **None** displays all entries.
Count Sessions and Count Bytes	Determines whether to display session or byte information.
	Determines whether the information is presented in a stacked column chart or a stacked area chart.
Export	Exports the graph as a .png image or as a PDF.
Bottom Bar	
	Indicates the period over which the change measurements are taken.

App Scope Traffic Map Report

The Traffic Map report shows a geographical view of traffic flows according to sessions or flows.

App Scope Traffic Map Report



Each traffic type is color-coded as indicated in the legend below the chart. This report contains the following options.

Traffic Map Report Options	Description
Top Bar	
Top 10	Determines the number of records with the highest measurement included in the chart.
Incoming traffic	Displays incoming traffic.
Outgoing traffic	Displays outgoing traffic.
Count Sessions and Count Bytes	Determines whether to display session or byte information.
Zoom In and Zoom Out	Zoom in and zoom out of the map.
Export	Export the graph as a .png image or as a PDF.
Bottom Bar	

Traffic Map Report Options	Description
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	Indicates the period over which the change measurements are taken.

Monitor > Session Browser

Select **Monitor** > **Session Browser** to browse and filter current running sessions on the firewall. For information on filtering options for this page, see Log Actions.

Monitor > Block IP List

You can configure the firewall to place IP addresses on the block list in several ways, including the following:

- Configure a DoS Protection policy rule with the Action to **Protect** and apply a Classified DoS Protection profile to the rule. The profile includes the Block Duration.
- Configure a Security policy rule with a Vulnerability Protection profile that uses a rule with the Action to **Block IP** and apply the rule to a zone.

The Block IP List is supported on PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls.

What do you want to know?	See:
What do the Block IP List fields indicate?	Block IP List Entries
How do I filter, navigate, or delete Block IP List entries?	View or Delete Block IP List Entries
Looking for more?	Set Up Antivirus, Anti-Spyware, and VulnerabilityProtection DoS Protection Against Flooding of New Sessions Monitor Blocked IP Addresses

Block IP List Entries

- **Monitor** > **BlockIPList**

The following table explains the block list entry for a source IP address that the firewall is blocking.

Field	Description
Block Time	Month/day and hours:minutes:seconds when the IP address went on the Block IP List.
Type	Type of block action: whether the hardware (hw) or software (sw) blocked the IP address. When you configure a DoS Protection policy or a Security policy that uses a Vulnerability Protection profile to block connections from source IPv4 addresses, the firewall automatically blocks that traffic in hardware before those packets use CPU or packet buffer resources. If attack traffic exceeds the blocking capacity of the hardware, the firewall uses software to block the traffic.
Source IP Address	Source IP address of the packet that the firewall blocked.
Ingress Zone	Security zone assigned to the interface where the packet entered the firewall.
Time Remaining	Number of seconds remaining for the IP address to be on the Block IP List.

Field	Description
Block Source	Name of the classified DoS Protection profile or Vulnerability protection object name where you specified the Block IP action.
Total Blocked IPs: x out of y (z% used)	Count of blocked IP addresses (x) out of the number of blocked IP addresses the firewall supports (y), and the corresponding percentage of blocked IP addresses used (z).

View or Delete Block IP List Entries

Navigate the Block IP list entries, view detailed information, and delete an entry if desired.

View or Delete Block IP List Entries	
Search for specific Block IP List information	Select a value in a column, which enters a filter in the **Filters** field, and click the right arrow to initiate the search for entries with that value. Click the X to remove the filter.
View Block IP List entries beyond the current screen	Enter a page number in the **Page** field or click the single arrows to see the Next Page or Previous Page of entries. Click the double arrows to view the Last Page or First Page of entries.
View detailed information about an IP address on the Block IP List	Click on a Source IP Address of an entry, which links to Network Solutions Who Is with information about the address.
Delete Block IP List entries	Select an entry and click **Delete**. *Only deletion of Hardware entries is supported from the web interface. However, deleting both Hardware and Software entries is supported from the CLI.*
Clear the entire Block IP List	Click **Clear All** to permanently delete all entries, which means those packets are no longer blocked. *Only clearing the Block IP list of Hardware entries is supported from the web interface. However, clearing both Hardware and Software entries is supported from the CLI.*

Monitor > Botnet

The botnet report enables you to use behavior-based mechanisms to identify potential malware- and botnet-infected hosts in your network. The report assigns each host a confidence score of 1 to 5 to indicate the likelihood of botnet infection, where 5 indicates the highest likelihood. Before scheduling the report or running it on demand, you must configure it to identify types of traffic as suspicious. The PAN-OS® Administrator's Guide provides details on interpreting botnet report output.

- Botnet Report Settings
- Botnet Configuration Settings

Botnet Report Settings

- Monitor > Botnet > Report Setting

Before generating the botnet report, you must specify the types of traffic that indicate potential botnet activity (see Configuring the Botnet Report). To schedule a daily report or run it on demand, click **Report Setting** and complete the following fields. To export a report, select it and **Export to PDF**, **Export to CSV**, or **Export to XML**.

Botnet Report Settings	Description
Test Run Time Frame	Select the time interval for the report—**Last 24 Hours** (default) or **Last Calendar Day**.
Run Now	Click **Run Now** to manually and immediately generate a report. The report displays in a new tab within the Botnet Report dialog.
No. of Rows	Specify the number of rows to display in the report (default is 100).
Scheduled	Select this option to automatically generate the report daily. By default, this option is enabled.
Query Builder	(Optional) **Add** queries to the Query Builder to filter the report output by attributes such as source/destination IP addresses, users, or zones. For example, if you know that traffic initiated from the IP address 192.0.2.0 contains no potential botnet activity, you can add **`not (addr.src in 192.0.2.0)`** as a query to exclude that host from the report output. • **Connector**—Select a logical connector (**and** or **or**). If you select **Negate**, the report will exclude the hosts that the query specifies. • **Attribute**—Select a zone, address, or user that is associated with the hosts that the firewall evaluates for botnet activity. • **Operator**—Select an operator to relate the **Attribute** to a **Value**. • **Value**—Enter a value for the query to match.

Botnet Configuration Settings

- Monitor > Botnet > Configuration

To specify the types of traffic that indicate potential botnet activity, click **Configuration** on the right side of the **Botnet** page and complete the following fields. After configuring the report, you can run it on demand or schedule it to run daily (see Monitor > PDF Reports > Manage PDF Summary).

The default Botnet report configuration is optimal. If you believe the default values identify false positives, create a support ticket so Palo Alto Networks can reevaluate the values.

Botnet Configuration Settings	Description
HTTP Traffic	**Enable** and define the **Count** for each type of HTTP Traffic that the report will include. The **Count** values you enter are the minimum number of events of each traffic type that must occur for the report to list the associated host with a higher confidence score (higher likelihood of botnet infection). If the number of events is less than the **Count**, the report will display the lower confidence score or (for certain traffic types) won't display an entry for the host. • **Malware URL visit** (range is 2–1000; default is 5)—Identifies users communicating with known malware URLs based on malware and botnet URL filtering categories. • **Use of dynamic DNS** (range is 2–1000; default is 5)—Looks for dynamic DNS query traffic that might indicate malware, botnet communications, or exploit kits. Generally, using dynamic DNS domains is very risky. Malware often uses dynamic DNS to avoid IP address block lists. Consider using URL filtering to block such traffic. • **Browsing to IP domains** (range is 2–1000; default is 10)—Identifies users who browse to IP domains instead of URLs. • **Browsing to recently registered domains** (range is 2–1000; default is 5)—Looks for traffic to domains that were registered within the past 30 days. Attackers, malware, and exploit kits often use newly registered domains. • **Executable files from unknown sites** (range is 2–1000; default is 5)—Identifies executable files downloaded from unknown URLs. Executable files are a part of many infections and, when combined with other types of suspicious traffic, can help you prioritize host investigations.
Unknown Applications	Define the thresholds that determine whether the report will include traffic associated with suspicious Unknown TCP or Unknown UDP applications. • **Sessions Per Hour** (range is 1–3600; default is 10)—The report includes traffic that involves up to the specified number of application sessions per hour. • **Destinations Per Hour** (range is 1–3600; default is 10)—The report includes traffic that involves up to the specified number of application destinations per hour. • **Minimum Bytes** (range is 1–200; default is 50)—The report includes traffic for which the application payload equals or exceeds the specified size. • **Maximum Bytes** (range is 1–200; default is 100)—The report includes traffic for which the application payload is equal to or less than the specified size.

Botnet Configuration Settings	Description
IRC	Select this option to include traffic involving IRC servers.

Monitor > PDF Reports

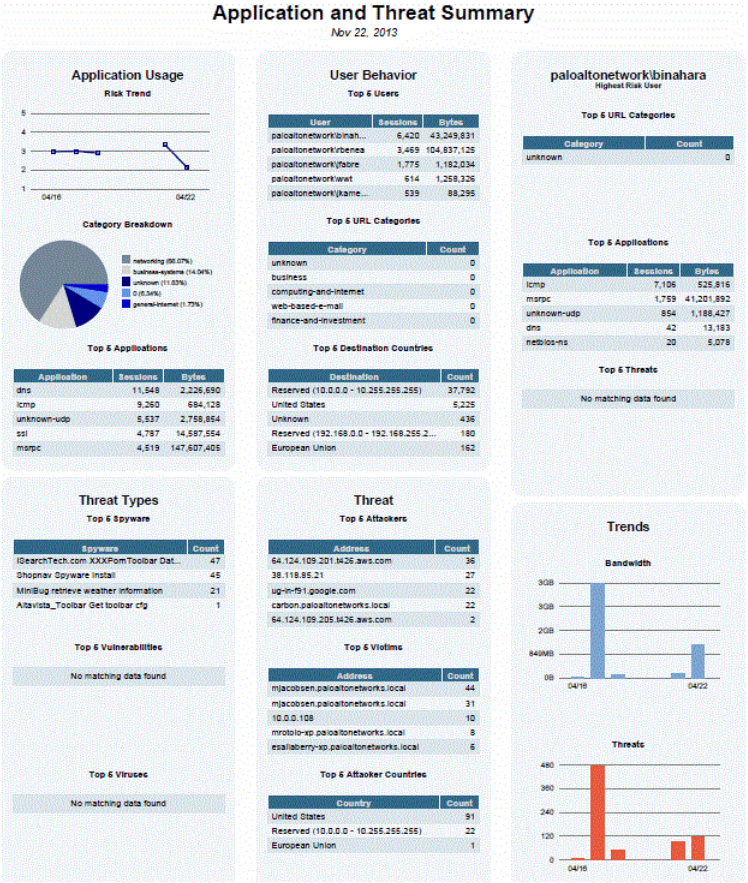
The following topics describe PDF reports.

- Monitor > PDF Reports > Manage PDF Summary
- Monitor > PDF Reports > User Activity Report
- Monitor > PDF Reports > SaaS Application Usage
- Monitor > PDF Reports > Report Groups
- Monitor > PDF Reports > Email Scheduler

Monitor > PDF Reports > Manage PDF Summary

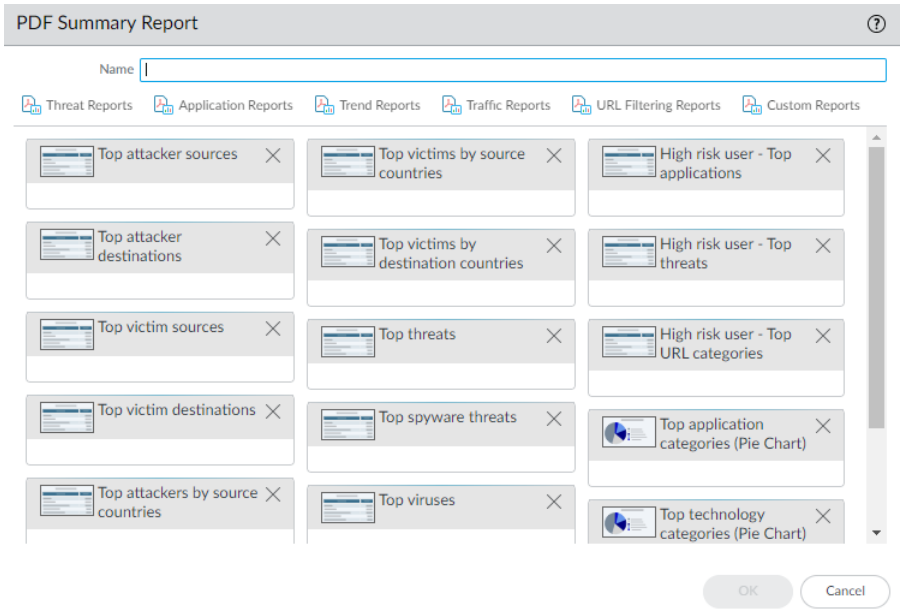
PDF summary reports contain information compiled from existing reports, based on data for the top 5 in each category (instead of top 50). They also contain trend charts that are not available in other reports.

PDF Summary Report



To create PDF summary reports, click **Add**. The **PDF Summary Report** page opens to show all of the available report elements.

Managing PDF Reports



Use one or more of these options to design the report:

- To remove an element from the report, click delete ([X]) or clear the item from the appropriate drop-down.
- Select additional elements by selecting them in the appropriate drop-down.
- Drag and drop an element to move it to another area of the report.

There is a maximum of 18 report elements allowed. If you have 18 already, you must delete existing elements before you can add new ones.

To **Save** the report, enter a report name, and click **OK**.

To display PDF reports, select **Monitor** > **Reports**, click **PDF Summary Report** to select a report, and click a day in the calendar to download a report for that day.

New PDF summary reports will not appear until after the report runs, which will occur automatically every 24 hours at 2 a.m.

Monitor > PDF Reports > User Activity Report

Use this page to create reports that summarize the activity of individual users or user groups. Click **Add** and specify the following information.

User/Group Activity Report Settings	Description
Name	Enter a name to identify the report (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Type	For User Activity Report: Select **User** and enter the **Username** or **IP address** (IPv4 or IPv6) of the user who will be the subject of the report.
	For Group Activity Report: Select **Group** and enter the **Group Name**.

User/Group Activity Report Settings	Description
Additional Filters	Select **Filter Builder** to create filters for the User/Group Activity Report.
Time Period	Select the time frame for the report from the drop-down.
Include Detailed Browsing	(Optional) Select this option to include detailed URL logs in the report. *The detailed browsing information can include a large volume of logs (thousands) for the selected user or user group and cause a report to be very large.*

The Group Activity Report does not include Browsing Summary by URL Category; all other information is common across the User Activity Report and the Group Activity Report.

To run the report on demand, click **Run Now**. To change the maximum number of rows that display in the report, see Logging and Reporting Settings.

To save the report, click **OK**. You can then schedule the report for email delivery (Monitor > PDF Reports > Email Scheduler).

Add a Log Filter

Build log filters to the User Activity and Group Activity Reports to customize reports. You can filter activity reports based on application, application characteristics and more. For example, if you have are interested in a SaaS application that don't have certifications, you can build a filter based on this application characteristic.

Add Log Filter Field	Description
Log Filter Text Box	Write the filter you would like to apply to the log. You can write multiple filters.
Connector	Append the filter with an additional filtering option. Check the **Negate** box to not apply a connector the filter you wrote.
Attribute	Select the attribute you wold like to append from the menu.
Operator	Select whether Attribute should equal or not equal the Value.
Value	Set the Value for the attribute. When available, a drop-down menu with possible values will be available.

Select **Apply** to apply the built filter to the User Activity or Group Activity Report.

Monitor > PDF Reports > SaaS Application Usage

Use this page to generate a SaaS application usage report that summarizes the security risks associated with the SaaS applications traversing your network. This predefined report presents a comparison of the sanctioned versus unsanctioned applications, summarizes the risky SaaS applications with unfavorable hosting characteristics, and highlights the activity, usage, and compliance of the applications by listing the top applications for each category on the detailed pages. You can use this detailed risk information to enforce policy for SaaS applications that you want to allow or block on your network.

For generating an accurate and informative report, you must tag the sanctioned applications on your network (see Generate the SaaS Application Usage Report). The firewall and Panorama consider any application without this predefined tag as unsanctioned for use on the network. It is important to know about the sanctioned applications and unsanctioned applications that are prevalent on your network because unsanctioned SaaS applications are a potential threat to information security; they are not approved for use on your network and can cause an exposure to threats and loss of private and sensitive data.

Make sure you tag applications consistently across all firewalls or device groups. If the same application is tagged as sanctioned in one virtual system and is not sanctioned in another—or on Panorama, if an application is unsanctioned in a parent device group but is tagged as sanctioned in a child device group (or vice versa)—the SaaS Application Usage report will produce overlapping results.

On the ACC, set the Application View to By Sanctioned State to visually identify applications that have different sanctioned state across virtual systems or device groups. Green indicates sanctioned applications, blue is for unsanctioned applications, and yellow indicates applications that have a different sanctioned state across different virtual systems or device groups.

To configure the report, click **Add** and specify the following information:

SaaS Application Usage Report Settings	Description
Name	Enter a name to identify the report (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Time Period	Select the time frame for the report from the drop-down. The report includes data from the current day (the day on which the report is generated).
Include logs from	From the drop-down, select whether you want to generate the report on a selected user group, on a selected zone, or for all user groups and zones configured on the firewall or Panorama. • **For a selected user group**—Select the **User Group** for which the firewall or Panorama will filter the logs. • **For a selected zone**—Select the **Zone** for which the firewall or Panorama will filter the logs. • **For all user groups and zones**—You can report on all groups or choose up to 25 user groups for which you want visibility. If you have more than 25 groups, the firewall or Panorama will display the top 25 groups in the report and assign all remaining user groups to the Others group.

SaaS Application Usage Report Settings	Description
Include user group information in the report (Not available if you choose to generate the report on a **Selected User Group**.)	This option filters the logs for the user groups you want to include in the report. Select the **manage groups** or the **manage groups for the selected zone** link to choose up to 25 user groups for which you want visibility. When you generate a report for specific user groups on a selected zone, users who are not a member of any of the selected groups are assigned to a user group called Others.
User group	Select the user group(s) for which you want to generate the report. This option displays only when you choose **Selected User Group** in the **Include logs from** drop-down.
Zone	Select the zone for which you want to generate the report. This option displays only when you choose **Selected Zone** in the **Include logs from** drop-down. You can then select include user group information in the report.
Include detailed application category information in report	The SaaS Application Usage PDF report is a two-part report. By default, both parts of the report are generated. The first part of the report (ten pages) focuses on the SaaS applications used on your network during the reporting period. Clear this option if you do not want the second part of the report that includes detailed information for SaaS and non-SaaS applications for each application subcategory listed in the first part of the report. This second part of the report includes the names of the top applications in each subcategory and information about users, user groups, files, bytes transferred, and threats generated from these applications. Without the detailed information, the report is ten-pages long.
Limit max subcategories in the report to	Select whether you want to use all application subcategories in the SaaS Application Usage report or whether you want to limit the maximum number to 10, 15, 20, or 25 subcategories. When you reduce the maximum number of subcategories, the detailed report is shorter because you limit the SaaS and non-SaaS application activity information included in the report.

Click **Run Now** to generate the report on demand.

You can generate this report on demand or you can schedule it to run on a daily, weekly, or monthly cadence. To schedule the report, see schedule reports for email delivery.

On PA-220 and PA-220R firewalls, the SaaS Application Usage report is not sent as a PDF attachment in the email. Instead, the email includes a link you use to open the report in a web browser.

For more information on the report, see Manage Reporting.

Monitor > PDF Reports > Report Groups

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Report Group Settings	Description
Name	Enter a name to identify the report group (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Title Page	Select this option to include a title page in the report.
Title	Enter the name that will appear as the report title.
Report selection / Widgets	For each report to include in the group, select the report in the left column and **Add** it to the right column. You can select the following report types: • Predefined Report • Custom Report • PDF Summary Report • CSV • Log View—Whenever you create a custom report, the firewall automatically creates a Log View report with the same name. The Log View report shows the logs that the firewall used to build the contents of the custom report. To include the log view data, when creating a report group, add your **Custom Reports** and then add the matching **Log View** reports. The aggregate report generated for the report group displays the custom report data followed by the log data. After you save the report group, the Widgets column of the Report Groups page lists the reports you added to the group.

To use the report group, refer to Monitor > PDF Reports > Email Scheduler.

Monitor > PDF Reports > Email Scheduler

Use the Email scheduler to schedule reports for delivery by email. Before adding a schedule, you must define report groups and an email profile. Refer to Monitor > PDF Reports > Report Groups and Device > Server Profiles > Email.

Scheduled reports begin running at 2:00 AM, and email forwarding occurs after all scheduled reports have finished running.

Email Scheduler Settings	Description
Name	Enter a name to identify the schedule (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

Email Scheduler Settings	Description
Report Group	Select the report group (Monitor > PDF Reports > Report Groups) or the SaaS Application Usage report (Monitor > PDF Reports > SaaS Application Usage) you want to schedule.
Email Profile	Select the profile that defines the email settings. Refer to Device > Server Profiles > Email for information on defining email profiles.
Recurrence	Select the frequency at which to generate and send the report.
Override Email Addresses	Enter an optional email address to use instead of the recipient specified in the email profile.
Send test email	Click to send a test email to the email address defined in the selected **Email Profile**.

Monitor > Manage Custom Reports

You can create custom reports to run on demand or on schedule (each night). For predefined reports, select **Monitor** > **Reports**.

After the firewall has generated a scheduled custom report, you risk invalidating the past results of that report if you modify its configuration to change its future output. If you need to modify a scheduled report configuration, the best practice is to create a new report.

Add a custom report to create a new one. To base the report on an existing template, **Load Template** and select the template. To generate a report on demand, instead of or in addition to the **Scheduled** time, click **Run Now**. Specify the following settings to define the report.

Custom Report Settings	Description
Name	Enter a name to identify the report (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the custom report.
Database	Choose the database to use as the data source for the report.
Scheduled	Select this option to run the report each night. The report then becomes available by selecting **Monitor** > **Reports**.
Time Frame	Choose a fixed time frame or choose **Custom** and specify a date and time range.
Sort By	Choose sorting options to organize the report, including the amount of information to include in the report. The available options depend on the choice of database.
Group By	Choose grouping options to organize the report, including the amount of information to include in the report. The available options depend on the choice of database.
Columns	Select Available Columns to include in the custom report and add (⊕) them to Selected Columns. Select **Up**, **Down**, **Top**, and **Bottom** to reorder selected columns. As needed, you can also select and remove (⊖) previously selected columns.
Query Builder	To build a report query, specify the following and click **Add**. Repeat as needed to construct the full query. • **Connector**—Choose the connector (**and** or **or**) to precede the expression you are adding. • **Negate**—Select this option to interpret the query as a negation. In the previous example, the negate option causes a match on entries that are not in the past 24 hours or are not from the untrust zone. • **Attribute**—Choose a data element. The available options depend on the choice of database.

Custom Report Settings	Description
	• **Operator**—Choose the criterion to determine whether the attribute applies (such as =). The available options depend on the choice of database. • **Value**—Specify the attribute value to match.

For more information, see Generate Custom Reports.

Monitor > Reports

The firewall provides various “top 50” reports of the traffic statistics for the previous day or a selected day in the previous week.

To view a report, expand a report category (such as Custom Reports) on the right side of the page and select a report name. The page lists reports in sections. You can view the information in each report for the selected time period.

By default, the firewall displays all reports for the previous calendar day. To view reports for other dates, select a report generation date in the calendar at the bottom right of the page.

To view reports on a system other than the firewall, select an export option:

- **Export to PDF**
- **Export to CSV**
- **Export to XML**

Policies

The following topics describe firewall policy types, how to move or clone policies, and describes policy settings:

- Policy Types
- Move or Clone a Policy Rule
- Audit Comment Archive
- Rule Usage Hit Count Query
- Policies > Security
- Policies > NAT
- Policies > QoS
- Policies > Policy Based Forwarding
- Policies > Decryption
- Policies > Tunnel Inspection
- Policies > Application Override
- Policies > Authentication
- Policies > DoS Protection
- Policies > SD-WAN

Policy Types

Policies enable you to control firewall operation by enforcing rules and automating actions. The firewall supports the following policy types:

- Basic security policies to block or allow a network session based on the application, the source and destination zones and addresses, and—optionally—based on the service (port and protocol). Zones identify the physical or logical interfaces that send or receive the traffic. See Policies > Security.
- Network Address Translation (NAT) policies to translate addresses and ports. See to Policies > NAT.
- Quality of Service (QoS) policies to determine how traffic is classified for treatment when it passes through an interface with QoS enabled. See Policies > QoS.
- Policy-based forwarding policies to override the routing table and specify an egress interface for traffic. See Policies > Policy Based Forwarding.
- Decryption policies to specify traffic decryption for security policies. Each policy can specify the categories of URLs for the traffic you want to decrypt. SSH decryption is used to identify and control SSH tunneling in addition to SSH shell access. See Policies > Decryption.
- Tunnel Inspection policies to enforce Security, DoS Protection, and QoS policies on tunneled traffic, and to view tunnel activity. See Policies > Tunnel Inspection.
- Override policies to override the application definitions provided by the firewall. See Policies > Application Override.
- Authentication policies to define authentication for end users who access network resources. See Policies > Authentication.
- Denial of service (DoS) policies to protect against DoS attacks and take protective action in response to rule matches. See Policies > DoS Protection.
- SD-WAN policies to determine link path management between the source and destination zones when link path health degrades below the approved, configured health metrics. See Policies > SD-WAN.

Shared polices pushed from Panorama™ display in orange on the firewall web interface. You can edit these shared policies only on Panorama; you cannot edit them on the firewall.

View Rulebase as Groups to view all the tag groups used in a rulebase. In rule bases with many rules, viewing the rulebase as groups simplifies the display by presenting the tags, color code, and the number of rules in each group while preserving the established rule hierarchy.

Move or Clone a Policy Rule

When moving or cloning policies, you can assign a **Destination** (a virtual system on a firewall or a device group on Panorama) for which you have access permissions, including the Shared location.

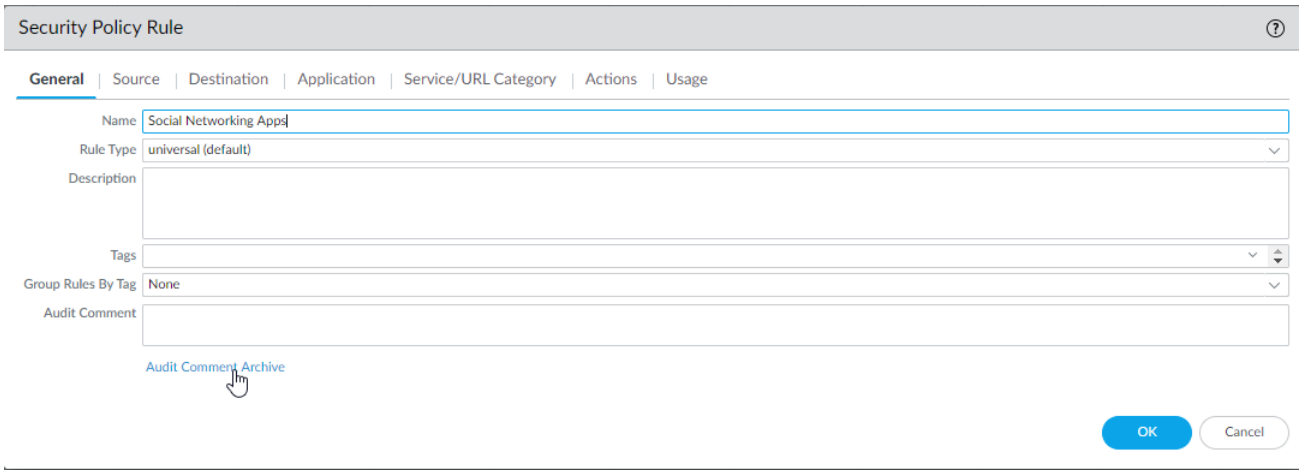
To move a policy rule, select the rule in the **Policies** tab, click **Move**, select **Move to other vsys** (firewalls only) or **Move to different rulebase or device group** (Panorama only), specify the fields in the following table, and then click **OK**.

To clone a policy rule, select the rule in the **Policies** tab, click **Clone**, specify the fields in the following table, and then click **OK**.

Move/Clone Settings	Description
Selected Rules	Displays the Name and current Location (virtual system or device group) of the policy rules you selected for the operation.
Destination	Select the new location for the policy or object: a virtual system, device group, or Shared. The default value is the **Virtual System** or **Device Group** that you selected in the **Policies** or **Objects** tab.
Rule order	Select the rule position relative to other rules: • **Move top**—The rule will precede all other rules. • **Move bottom**—The rule will follow all other rules. • **Before rule**—In the adjacent drop-down, select the subsequent rule. • **After rule**—In the adjacent drop-down, select the preceding rule.
Error out on first detected error in validation	Select this option (selected by default) to make the firewall or Panorama display the first error it finds and stop checking for more errors. For example, an error occurs if the **Destination** doesn't include an object that is referenced in the policy rule you are moving. If you clear this selection, the firewall or Panorama will find all errors before displaying them.

Audit Comment Archive

Select the **Audit Comment Archive** to view the audit comment history, configuration logs, and the rule change history of a selected rule.



- Audit Comments
- Config Logs (between commits)
- Rule Changes

Audit Comments

View the **Audit Comment** history for a selected policy rule. Apply and save filters to quickly identify specific audit comments and to export the displayed audit comments in CSV format.

Field	Description
Commit Time	Time when the audit comment was committed.
Audit Comment	Contents of the audit comment.
Administrator	User who added or changed the audit comment.
Config Version	Configuration revision version. 0 indicates the first time the policy rule was created and committed to Panorama.

Config Logs (between commits)

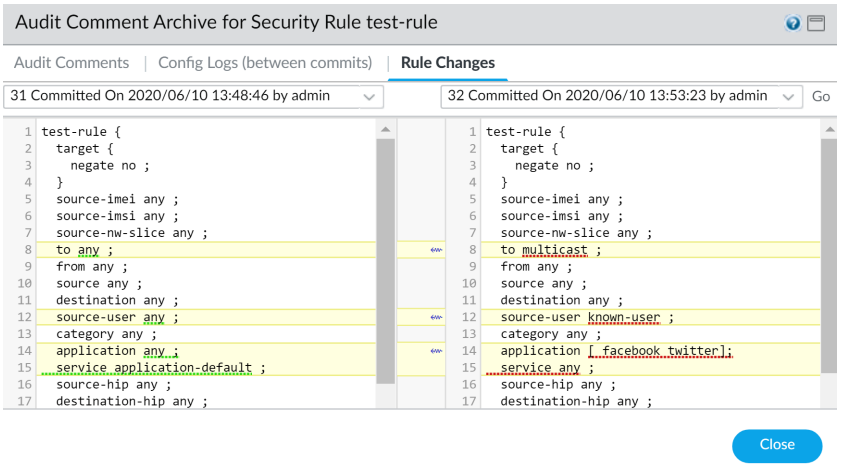
View the configuration log generated by the selected policy rule between commits. Apply and save filters to quickly identify specific config logs and to export the displayed config logs in CSV format.

Field	Description
Time	Time when the audit comment was committed.

Field	Description
Administrator	Contents of the audit comment.
Command	Type of command executed.
Before Change	Rule information before the change occurred. For example; if you rename a rule, the previous name is displayed.
After Change	Rule information after the change occurred. For example, if you rename a rule, the new name is displayed.
Device Name	Name of the device before audit comment change.

Rule Changes

View and compare configuration version of the selected policy rule to analyze what changes occurred. In the drop-down, select the two policy rule config versions you want to compare.



Rule Usage Hit Count Query

- **Policies** > **Rule Usage**

Use the rule usage query to filter the selected rulebase over a specified period of time. The rule usage query allows you to quickly filter your policy rulebase to identify unused rules for removal so that you can reduce open entry points for an attacker. Click **PDF/CSV** to export the filtered rules in PDF or CSV format. To use the Rule Usage Hit Count Query, you must enable the **Policy Rule Hit Count** setting (Device > Setup > Management).

By default, the **Name**, **Location**, **Created**, **Modified**, and **Rule Usage** columns are displayed when you query the rule usage in your policy rule base. You can add more columns to view additional information about the policy rules.

Task	Description
Hit Count	
Timeframe	Indicate the time frame to query the selected rulebase. Select from the predetermined time frames or set a **Custom** time frame.
Usage	Select the rule usage to query: **Any**, **Unused**, **Used**, or **Partially Used** (Panorama only).
Since	(Custom Timeframe only) Select the date and time from which to query the policy rulebase.
Exclude rules reset during the last _ days	Select this option to exclude any rules that were manually reset by a user within the specified number of days.
Actions	
Delete	Delete one or more selected policy rules.
Enable	Enable one or more selected policy rules when disabled.
Disable	Disable one or more selected policy rules.
PDF/CSV	Export the filtered policy rules currently displayed in PDF or CSV format.
Reset Rule Hit Counter	Reset the rule usage data for the **Selected rules** or for **All rules** that have been filtered and are currently displayed.
Tag	Apply one or more group tags to one or more selected policy rules. The group tag must already exist in order to tag the policy rule(s).
Untag	Remove one or more group tags from one or more selected policy rules.

Device Rule Usage for Rule Hit Count Query

You can view the device and virtual system rule usage when you viewing the rule usage for a policy rule from the Panorama management server. **Reset Rule Hit Counter** to reset the Hit Count, First Hit, and Last Hit.

Click **PDF/CSV** to export the filtered rules in PDF or CSV format.

Field	Description
Device Group	Device group that device or virtual system belongs to.
Device Name/Virtual System	Name of the device group or virtual system.
Hit Count	Total number of traffic matches for the policy rule.
Last Hit	Date and time of the latest traffic match for the policy rule.
First Hit	Date and time of the first traffic match for the policy rule.
Last Update Received	Date and time of the last received rule usage information from the device to the Panorama management server.
Created	Date and time the policy rule was created.
Modified	Date and time the policy rule was last modified. Column is blank if the policy rule has not been modified.
State	Connection status of the device: `Connected`, or `Disconnected`.

Policies > Security

Security policy rules reference security zones and enable you to allow, restrict, and track traffic on your network based on the application, user or user group, and service (port and protocol). By default, the firewall includes a security rule named *rule1* that allows all traffic from the Trust zone to the Untrust zone.

What do you want to know?	See:
What is a Security policy?	Security Policy Overview For Panorama, see Move or Clone a Policy Rule
What are the fields available to create a Security policy rule?	Building Blocks in a Security Policy Rule
How can I use the web interface to manage Security policy rules?	Creating and Managing Policies Overriding or Reverting a Security Policy Rule Applications and Usage Security Policy Optimizer
Looking for more?	Security Policy

Security Policy Overview

Security policies allow you to enforce rules and take action, and can be as general or specific as needed. The policy rules are compared against the incoming traffic in sequence, and because the first rule that matches the traffic is applied, the more specific rules must precede the more general ones. For example, a rule for a single application must precede a rule for all applications if all other traffic-related settings are the same.

To ensure that end users authenticate when they try to access your network resources, the firewall evaluates Authentication policy before Security policy. For details, see Policies > Authentication.

For traffic that doesn't match any user-defined rules, the default rules apply. The default rules—displayed at the bottom of the security rulebase—are predefined to allow all intrazone traffic (within the zone) and deny all interzone traffic (between zones). Although these rules are part of the predefined configuration and are read-only by default, you can **Override** them and change a limited number of settings, including the tags, action (allow or deny), log settings, and security profiles.

The interface includes the following tabs for defining Security policy rules.

- **General**—Select the **General** tab to configure a name and description for the Security policy rule.
- **Source**—Select the **Source** tab to define the source zone or source address from which the traffic originates.
- **User**—Select the **User** tab to enforce policy for individual users or a group of users. If you are using GlobalProtect™ with host information profile (HIP) enabled, you can also base the policy on information collected by GlobalProtect. For example, the user access level can be determined HIP that notifies the firewall about the user's local configuration. The HIP information can be used for granular access control based on the security programs that are running on the host, registry values, and many other checks such as whether the host has antivirus software installed.

- **Destination**—Select the **Destination** tab to define the destination zone or destination address for the traffic.
- **Application**—Select the **Application** tab to have the policy action occur based on an application or application group. An administrator can also use an existing App-ID™ signature and customize it to detect proprietary applications or to detect specific attributes of an existing application. Custom applications are defined in **Objects** > **Applications**.
- **Service/URL Category**—Select the **Service/URL Category** tab to specify a specific TCP and/or UDP port number or a URL category as match criteria in the policy.
- **Actions**—Select the **Actions** tab to determine the action that will be taken based on traffic that matches the defined policy attributes.
- **Target**—Select the **Target** tab to specify devices or tags for the security policy rule.
- **Usage**—Select the **Usage** tab to view a rule's usage, including the number of applications seen on a rule, when the last new applications was seen on the rule, hit count data, traffic over the past 30 days, and when the rule was created and last edited.

Building Blocks in a Security Policy Rule

- Policies > Security

The following section describes each component in a Security policy rule. When you create a Security policy rule, you can configure the options described here.

Building Blocks in a Security Rule	Configured In	Description
Rule number	N/A	The firewall automatically numbers each rule and the order of the rules will change as rules are moved. When you filter rules to match specific filters, each rule displays with its number in the context of the complete set of rules in the rulebase and its place in the evaluation order. Panorama independently numbers pre-rules and post-rules. When Panorama pushes rules to a managed firewall, the rule numbering incorporates hierarchy in pre-rules, firewall rules, and post-rules within a rulebase and reflects the rule sequence and its evaluation order.
Name	**General**	Enter a name to identify the rule. The name is case-sensitive and can have up to 63 characters, which can be letters, numbers, spaces, hyphens, and underscores. The name must be unique on a firewall and, on Panorama, unique within its device group and any ancestor or descendant device groups.
Rule Type		Specifies whether the rule applies to traffic within a zone, between zones, or both: • **universal** (default)—Applies the rule to all matching interzone and intrazone traffic in the specified source and destination zones. For example, if you create a universal rule with source zones A and B and destination zones A and B, the rule would apply to all traffic within zone A, all traffic within zone B, and all traffic from zone A to zone B and all traffic from zone B to zone A. • **intrazone**—Applies the rule to all matching traffic within the specified source zones (you cannot specify a

Building Blocks in a Security Rule	Configured In	Description
		destination zone for intrazone rules). For example, if you set the source zone to A and B, the rule would apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B. • **interzone**—Applies the rule to all matching traffic between the specified source and destination zones. For example, if you set the source zone to A, B, and C and the destination zone to A and B, the rule would apply to traffic from zone A to zone B, from zone B to zone A, from zone C to zone A, and from zone C to zone B, but not traffic within zones A, B, or C.
Description		Enter a description for the policy (up to 1,024 characters).
Tags		Specify the tag for the policy. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain rules with specific words like Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location. You can also add tags to the default rules.
Source Zone	**Source**	**Add** source zones (default is **Any**). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.
Source Address	**Source**	**Add** source addresses, address groups, or regions (default is **Any**). Select from the drop-down or select **Address** object, **Address Group**, or **Regions** (bottom of the drop-down) to specify the settings. Objects>Addresses and Objects>AddressGroups describe the types of address objects and address groups, respectively, that a Security policy rule supports. Selecting the **Negate** option will apply the rule to source addresses from the specified zone except for the addresses specified.
Source User	**Source**	**Add** the source users or groups of users subject to the policy: • **any**—Includes any traffic regardless of user data. • **pre-logon**—Includes remote users that are connected to the network using GlobalProtect, but are not logged into

Building Blocks in a Security Rule	Configured In	Description
		their system. When the Pre-logon option is configured on the Portal for GlobalProtect endpoints, any user who is not currently logged into their machine will be identified with the username pre-logon. You can then create policies for pre-logon users and although the user is not logged in directly, their machines are authenticated on the domain as if they were fully logged in. • **known-user**—Includes all authenticated users, which means any IP address with user data mapped. This option is equivalent to the domain users group on a domain. • **unknown**—Includes all unauthenticated users, which means IP addresses that are not mapped to a user. For example, you could use **unknown** for guest level access to something because they will have an IP address on your network but will not be authenticated to the domain and will not have IP address-to-user mapping information on the firewall. • **Select**—Includes selected users as determined by the selection in this window. For example, you may want to add one user, a list of individuals, some groups, or manually add users.  *If the firewall collects user information from a RADIUS, TACACS+, or SAML identity provider server and not from the User-ID™ agent, the list of users does not display; you must enter user information manually.*
Source Device	**Source**	**Add** the host devices subject to the policy: • **any**—Includes any device. • **no-hip**—HIP information is not required. This setting enables access from third-party devices that cannot collect or submit HIP information. • **quarantine**—Includes any device that is in the quarantine list (**Device** > **Device Quarantine**). • **select**—Includes selected devices as determined by your configuration. For example, you can add a device object based on model, OS, OS family, or vendor.
Source HIP Profile	**Source**	**Add** host information profiles (HIP) to enable you to collect information about the security status of your end hosts, such as whether they have the latest security patches and antivirus definitions installed. Using host information profiles for policy enforcement enables granular security that ensures that the remote hosts accessing your critical resources are adequately maintained and in adherence with your security standards before they are allowed to access your network resources. The following source HIP profiles are supported:

Building Blocks in a Security Rule	Configured In	Description
		• **any**—Includes any endpoint, regardless of HIP information. • **select**—Includes selected HIP profiles as determined by your configuration. For example, you can add one HIP profile, a list of HIP profiles, or you can add HIP profiles manually. • **no-hip**—HIP information is not required. This setting enables access from third-party clients that cannot collect or submit HIP information.
Source Subscriber	**Source**	**Add** one or more source subscribers in a 5G or 4G network using the following formats: • **Any** • (5G only) 5G Subscription Permanent Identifier (SUPI) including IMSI • IMSI (14 or 15 digits) • Range of IMSI values from 11 to 15 digits, separated by a hyphen • IMSI prefix of six digits, with an asterisk (*) as a wildcard after the prefix • EDL that specifies IMSIs
Source Equipment		**Add** one or more source equipment IDs in a 5G or 4G network using the following formats: • **Any** • (5G only) 5G Permanent Equipment Identifier (PEI) including International Mobile Equipment Identity (IMEI) • IMEI (11 to 16 digits long) • IMEI prefix of eight digits for Type Allocation Code (TAC) • EDL that specifies IMEIs
Network Slice	**Source**	**Add** one or more source network slices based on network slice service type (SST) in a 5G network, as follows: • **Standardized (predefined) SST** • **eMBB** (enhanced Mobile Broadband)—For faster speeds and high data rates, such as video streaming. • **URLLC** (Ultra-Reliable Low-Latency Communications)—For mission-critical applications that are sensitive to latency, such as critical IoT (healthcare, wireless payments, home control, and vehicle communication). • **MIoT** (Massive Internet of Things)—For example, smart metering, smart waste management, anti-theft, asset management, and location tracking. • **Network Slice SST - Operator-Specific**—You name and specify the slice. The format of the slice name is text followed by a comma (,) and a number (range is 128 to 255). For example, Enterprise Oil2,145.

Building Blocks in a Security Rule	Configured In	Description
Destination Zone	**Destination**	**Add** destination zones (default is **any**). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases. *On intrazone rules, you cannot define a Destination Zone because these types of rules match only traffic with a source and a destination within the same zone. To specify the zones that match an intrazone rule, you need to specify only the Source Zone.*
Destination Address		**Add** destination addresses, address groups, or regions (default is **Any**). Select from the drop-down or click **Address** object, **Address Group**, or **Regions** (bottom of the drop-down) to specify address settings. Objects>Addresses and Objects>AddressGroups describe the types of address objects and address groups, respectively, that a Security policy rule supports. Selecting the **Negate** option will apply the rule to destination addresses in the specified zone except for the addresses specified.
Destination Device		**Add** the host devices subject to the policy: • **any**—Includes any device. • **quarantine**—Includes any device that is in the quarantine list (**Device** > **Device Quarantine**). • **select**—Includes selected devices as determined by your configuration. For example, you can add a device object based on model, OS, OS family, or vendor.
Application	**Application**	**Add** specific applications for the Security policy rule. If an application has multiple functions, you can select the overall application or individual functions. If you select the overall application, all functions are included and the application definition is automatically updated as future functions are added. If you are using application groups, filters, or containers in the Security policy rule, you can view details of these objects by hovering over the object in the Application column, opening the drop-down, and selecting **Value**. This allows you to view application members directly from the policy without having to navigate to the **Object** tab.

Building Blocks in a Security Rule	Configured In	Description
		Always specify one or more applications so that only applications you want on your network are allowed, which reduces the attack surface and gives you greater control over network traffic. Don't set the application to any, which allows any application's traffic and increases the attack surface.
Service	**Service/URL Category**	Select the services that you want to limit to specific TCP or UDP port numbers. Choose one of the following from the drop-down: • **any**—The selected applications are allowed or denied on any protocol or port. • **application-default**—The selected applications are allowed or denied only on their default **ports defined by Palo Alto Networks®**. This option is recommended for allow policies because it prevents applications from running on unusual ports and protocols which, if unintentional, can be a sign of undesired application behavior and usage. *When you use this option, the firewall still checks for all applications on all ports, but applications are allowed only on their default ports and protocols.* *For most applications, use application-default to prevent the application from using non-standard ports or exhibiting other evasive behaviors. If the default port for the application changes, the firewall automatically updates the rule to the correct default port. For applications that use non-standard ports, such as internal custom applications, either modify the application or create a rule that specifies the non-standard ports and apply the rule only to the traffic that requires the application.* • **Select**—**Add** an existing service or choose **Service** or **Service Group** to specify a new entry. (Or select Objects > Services and Objects > Service Groups).
URL Category		Select URL categories for the security rule. • Choose **any** to allow or deny all sessions regardless of the URL category. • To specify a category, **Add** one or more specific categories (including custom categories) from the drop-

Building Blocks in a Security Rule	Configured In	Description
		down. Select Objects > External Dynamic Lists to define custom categories.
Action Setting	**Actions**	Select the **Action** the firewall takes on traffic that matches the attributes defined in a rule: • **Allow** (default)—Allows the matched traffic. • **Deny**—Blocks matched traffic and enforces the default *Deny Action* defined for the application that is denied. To view the deny action defined by default for an application, view the application details (**Objects** > **Applications**). Because the default deny action varies by application, the firewall could block the session and send a reset for one application while it silently drops the session for another application. • **Drop**—Silently drops the application. A TCP reset is not sent to the host or application unless you select **Send ICMP Unreachable**. • **Reset client**—Sends a TCP reset to the client-side device. • **Reset server**—Sends a TCP reset to the server-side device. • **Reset both client and server**—Sends a TCP reset to both the client-side and server-side devices. • **Send ICMP Unreachable**—Available only for Layer 3 interfaces. When you configure Security policy rule to drop traffic or to reset the connection, the traffic does not reach the destination host. In such cases, for all UDP traffic and for TCP traffic that is dropped, you can enable the firewall to send an ICMP Unreachable response to the source IP address from where the traffic originated. Enabling this setting allows the source to gracefully close or clear the session and prevents applications from breaking. To view the ICMP Unreachable Packet Rate configured on the firewall, view Session Settings (**Device** > **Setup** > **Session**). To override the default action defined on the predefined interzone and intrazone rules: see Overriding or Reverting a Security Policy Rule.
Profile Setting	**Actions**	To specify the additional checking that the firewall performs on packets that match the Security profile rule, select individual Antivirus, Vulnerability Protection, Anti-Spyware, URL Filtering, File Blocking, Data Filtering, WildFire Analysis, Mobile Network Protection, and SCTP Protection profiles. To specify a profile group rather than individual profiles, select the **Profile Type** to be **Group** and then select a **Group Profile**.

Building Blocks in a Security Rule	Configured In	Description
		To define new profiles or profile groups, click **New** next to the appropriate profile or select **New Group Profile**. You can also attach Security Profiles (or profile groups) to the default rules.
Log Setting and Other Settings	**Actions**	To generate entries in the local traffic log for traffic that matches this rule, select the following options: • **Log At Session Start** (disabled by default)—Generates a traffic log entry for the start of a session.  *Don't enable Log at Session Start except for troubleshooting purposes or for tunnel session logs to show active GRE tunnels in the ACC. Logging at the session end consumes fewer resources and identifies the exact application if the application changes after a few packets, for example, from facebook-base to facebook-chat.* • **Log At Session End** (enabled by default)—Generates a traffic log entry for the end of a session.  *If the session start or end entries are logged, drop and deny entries are also logged.* • **Log Forwarding Profile**—To forward the local traffic log and threat log entries to remote destinations, such as Panorama and syslog servers, select a **Log Forwarding Profile**.  *The generation of threat log entries is determined by the Security Profiles. Define New log profiles as needed (refer to Objects > Log Forwarding).*  *Create and enable Log Forwarding profiles to send logs to dedicated external storage devices. This preserves the logs because the firewall has limited log storage space and when the space is consumed, the firewall purges the oldest logs.* You can also modify the log settings on the default rules. Specify any combination of the following options: • **Schedule**—To limit the days and times when the rule is in effect, select a schedule from the drop-down. Define **New** schedules as needed (refer to Settings to Control Decrypted SSL Traffic). • **QoS Marking**—To change the Quality of Service (QoS) setting on packets matching the rule, select **IP DSCP** or

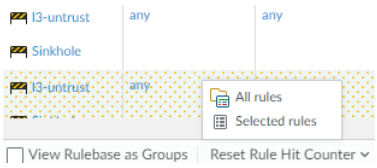
Building Blocks in a Security Rule	Configured In	Description
		IP Precedence and enter the QoS value in binary form or select a predefined value from the drop-down. For more information on QoS, refer to Quality of Service. • **Disable Server Response Inspection**—Disables packet inspection from the server to the client. The option is disabled by default.  *For the best security posture, do not enable Disable Server Response Inspection. With this option selected, the firewall only inspects the client-to-server flows. It does not inspect the server-to-client flows and therefore cannot identify if there are any threats in these traffic flows.*
Basics	**Rule Usage**	• **Rule Created**—Creation date and time of the rule. • **Last Edited**—The last date and time the rule was edited.
Activity	**Rule Usage**	• **Hit Count**—The total number of times traffic matched (hit) the rule. • **First Hit**—Time of the first rule match. • **Last Hit**—Time of the last rule match.
Applications	**Rule Usage**	• **Applications Seen**—The number of applications the rule allows. • **Last App Seen**—The number of days since the last new application (an application that wasn't previously seen) was seen on the rule. • **Compare Applications & Applications Seen**—Click to compare the applications configured on the rule against the applications seen on the rule. Use this tool to discover the applications that match the rule and to add applications to the rule.
Traffic (past 30 days)	**Rule Usage**	• **Bytes**—The amount of traffic on the rule over the past 30 days in bytes.  *A time period longer than 30 days would result in the oldest rules remaining at the top of the list because they are likely to have the most cumulative traffic. This can result in newer rules being listed below older rules even if the newer rules see heavy traffic.*
Any (target all devices) Panorama only	**Target**	Enable (check) to push the policy rule to all managed firewalls in the device group.

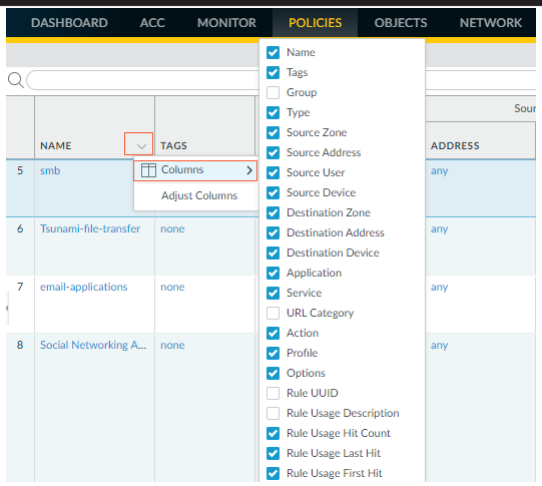
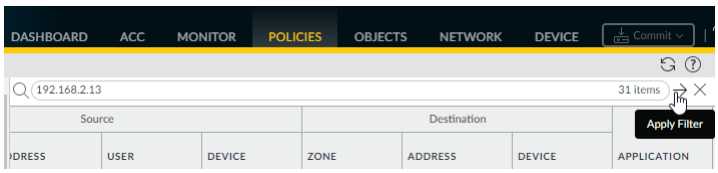
Building Blocks in a Security Rule	Configured In	Description
Devices Panorama only		Select one or more managed firewalls associated with the device group to push the policy rule to.
Tags Panorama only		**Add** one or more tags to push the policy rule to managed firewalls in the device group with the specified tag.
Target to all but these specified devices and tags Panorama only		Enable (check) to push the policy rule to all managed firewalls associated with the device group except for the selected device(s) and tag(s).

Creating and Managing Policies

Select the **Policies** > **Security** page to add, modify, and manage security policies:

Task	Description
Add	**Add** a new policy rule or select a rule on which to base a new rule and **Clone Rule**. The copied rule, "rule*n*" is inserted below the selected rule, where *n* is the next available integer that makes the rule name unique. For details on cloning, see Move or Clone a Policy Rule.
Modify	Select a rule to modify its settings. If the rule is pushed from Panorama, the rule is read-only on the firewall and you cannot edit it locally.
	Override and **Revert** actions pertain only to the default rules displayed at the bottom of the Security rulebase. These predefined rules—allow all intrazone traffic and deny all interzone traffic—instruct the firewall about how to handle traffic that does not match any other rule in the rulebase. Because they are part of the predefined configuration, you must **Override** them to edit select policy settings. If you are using Panorama, you can also **Override** the default rules and then push them to firewalls in a Device Group or Shared context. You can also **Revert** the default rules, which restores the predefined settings or the settings pushed from Panorama. For details, see Overriding or Reverting a Security Policy Rule.
Move	Rules are evaluated from the top down and as they are enumerated on the **Policies** page. To change the order in which the rules are evaluated against network traffic, select a rule and **Move Up**, **Move Down**, **Move Top**, **Move Bottom**, or **Move to a different rulebase or device group**. For details, see Move or Clone a Policy Rule.
Copy UUID	Copy the UUID of the rule to the clipboard for use when searching the configuration or the logs.
Delete	Select and **Delete** an existing rule.

Task	Description
Enable/Disable	To disable a rule, select and **Disable** it; to enable a rule that is disabled, select and **Enable** it.
Monitor Rule Usage	To identify rules that have not been used since the last time the firewall was restarted, **Highlight Unused Rules**. Unused rules have a dotted background. You can then decide whether to **Disable** a rule or **Delete** it. Rules not currently in use are displayed with a dotted yellow background. When policy rule hit count is enabled, the Hit Count data is used to determine whether a rule is unused. *Each firewall maintains a traffic flag for the rules that have a match. Because the flag is reset when a dataplane reset occurs on a reboot or a restart, it is best practice to monitor this list periodically to determine whether the rule had a match since the last check before you delete or disable it.* 
Reset rule Hit count	The **Hit Count** tracks the total traffic hits for the policy rule. The total traffic hit count persists through reboot, upgrade, and data plane restart. Alternatively, **Reset Rule Hit Counter** (bottom menu). To clear the hit count statistics, select **All Rules** or select specific rules and reset hit count statistics only for the **Selected rules**.  View the **First Hit** to identify when the Security policy was first hit. The date is formated as date hh:mm:ss year. You cannot reset this value. View the **Last Hit** to identify when the Security policy was last used. The date is formated as date hh:mm:ss year. You cannot reset this value.
Show/Hide columns	Show or hide the columns that display under **Policies**. Select the column name to toggle the display.

Task	Description
	
Apply filters	To apply a filter to the list, select from the **Filter Rules** drop-down. To define a filter, choose **Filter** from the item drop-down. *The default rules are not part of rulebase filtering and always show up in the list of filtered rules.*
	To view the network sessions that were logged as matches against the policy, choose **Log Viewer** from the rule name drop-down.
	To display the current value, choose **Value** from the entry drop-down. You can also edit, filter, or remove items directly from the column menu. For example, to view addresses included in an address group, hover over the object in the **Address** column and select **Value** from the drop-down. This allows you to quickly view the members and the corresponding IP addresses for the address group without having to navigate to the **Object** tab.
	To find objects used within a policy based on their name or IP address, use the filter. After you apply the filter, you will see only the items that match the filter. The filter also works with embedded objects. For example, when you filter on 10.1.4.8, only the policy that contains that address is displayed: 
Preview rules (Panorama only)	**Preview Rules** to view a list of the rules before you push the rules to the managed firewalls. Within each rulebase, the hierarchy of rules is visually demarcated for each device group (and managed firewall) to make it easier to scan through a large numbers of rules.
Export Configuration Table	Administrative roles with a minimum of read-only access can export the policy rulebase as **PDF/CSV**. You can apply filters to create more specific table configuration

Task	Description
	outputs as needed, such as for audits. Only visible columns in the web interface will be exported. See Configuration Table Export.
Highlight Unused Rule	Highlight any policy rule with no traffic matches in the **Rule Usage** column.
Group	Manage tag groups when you have the **View Rulebase as Groups** box checked. You can perform the following actions: • **Move rules in group to different rulebase or device group**—Move the selected tag group to a different device group. • **Change group of all rules**—Move the rules in the selected tag group to a different tag group in the rulebase. • **Delete all rules in group**—Deletes all rules in the selected tag group. • **Clone all rules in group**—Clones the rules in the selected tag group to a device group.
View Rulebase as Groups	**View Rulebase as Groups** to view the policy rulebase using the tag used in **Group Rules by Tag** . The visible policy rules are those which belong to the selected tag group.
Test Policy Match	Perform a test of the protection policies for the selected policy rulebase to verify that the correct traffic is denied and allowed.

Overriding or Reverting a Security Policy Rule

The default security rules—interzone-default and intrazone-default—have predefined settings that you can override on a firewall or on Panorama. If a firewall receives the default rules from a device group, you can also override the device group settings. The firewall or virtual system where you perform the override stores a local version of the rule in its configuration. The settings you can override are a subset of the full set (the following table lists the subset for security rules). For details on the default security rules, see Policies > Security.

To override a rule, select **Policies** > **Security** on a firewall or **Policies** > **Security** > **Default Rules** on Panorama. The Name column displays the inheritance icon ( ) for rules you can override. Select the rule, click **Override**, and edit the settings in the following table.

To revert an overridden rule to its predefined settings or to the settings pushed from a Panorama device group, select **Policies** > **Security** on a firewall or **Policies** > **Security** > **Default Rules** on Panorama. The Name column displays the override icon ( ) for rules that have overridden values. Select the rule, click **Revert**, and click **Yes** to confirm the operation.

Fields to Override a Default Security Rule	Description
General Tab	
Name	The **Name** that identifies the rule is read-only; you cannot override it.
Rule Type	The **Rule Type** is read-only; you cannot override it.

Fields to Override a Default Security Rule	Description
Description	The **Description** is read-only; you cannot override it.
Tag	Select **Tags** from the drop-down. A policy tag is a keyword or phrase that enables you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you might want to tag certain security policies with Inbound to DMZ, tag specific decryption policies with the words Decrypt or No-decrypt, or use the name of a specific data center for policies associated with that location.
Actions Tab	
Action Setting	Select the appropriate **Action** for traffic that matches the rule. • **Allow**—(default) Allows the traffic. • **Deny**—Blocks traffic and enforces the default Deny Action that is defined for the application that the firewall is denying. To view the deny action that is defined by default for an application, view the application details in **Objects** > **Applications**. • **Drop**—Silently drops the application. The firewall does not send a TCP reset message to the host or application. • **Reset client**—Sends a TCP reset message to the client-side device. • **Reset server**—Sends a TCP reset message to the server-side device. • **Reset both**—Sends a TCP reset message to both the client-side and server-side devices.
Profile Setting	**Profile Type**—Assign profiles or profile groups to the security rule: • To specify the checking that the default security profiles perform, select **Profiles** and then select one or more of the individual **Antivirus**, **Vulnerability Protection**, **Anti-Spyware**, **URL Filtering**, **File Blocking**, **Data Filtering**, **WildFire Analysis**, **SCTP Protection**, and **Mobile Network Protection** profiles. • To assign a profile group rather than individual profiles, select **Group** and then select a **Group Profile** from the drop-down. • To define new profiles (Objects > Security Profiles) or profile groups, click **New** in the drop-down for the corresponding profile or group profile.
Log Setting	Specify any combination of the following options: • **Log Forwarding**—To forward the local traffic log and threat log entries to remote destinations, such as Panorama and syslog servers, select a **Log Forwarding** profile from the drop-down. Security profiles determine the generation of Threat log entries. To define a new **Log Forwarding** profile, select **Profile** in the drop-down (see Objects > Log Forwarding). • To generate entries in the local traffic log for traffic that matches this rule, select the following options:

Fields to Override a Default Security Rule	Description
	• **Log at Session Start**—Generates a traffic log entry for the start of a session (selected by default). • **Log at Session End**—Generates a traffic log entry for the end of a session (cleared by default).  *If you configure the firewall to include session start or session end entries in the Traffic log, it will also include drop and deny entries.*

Applications and Usage

- Policies > Security > Policy Optimizer > No App Specified > Compare (or click the number in **Apps Seen)**
- Policies > Security > Policy Optimizer > Unused Apps > Compare (or click the number in **Apps Seen)**
- Policies > Security and click the number in **Apps Seen**

On the Usage tab of the Security policy rule, you can also **Compare Applications** & **Applications Seen** to access tools that help you to migrate from port-based Security policy rules to application-based Security policy rules and to eliminate unused applications from rules in **Applications & Usage**.

Field	Description
Timeframe	The time period for the application information: • **Anytime**—Displays applications seen over the lifetime of the rule. • **Past 7 days**—Displays only applications seen over the last 7 days. • **Past 15 days**—Displays only applications seen over the last 15 days. • **Past 30 days**—Displays only applications seen over the last 30 days.
Apps on Rule	The applications configured on the rule or **Any** if no specific applications are configured on the rule. You can **Browse**, **Add**, and **Delete** applications as needed, and applications are configured on a rule, the circled number next to Apps on Rule indicates how many. Adding applications from this location is the same as adding applications on the Security policy rule **Application** tab.
Apps Seen	All applications seen and allowed on the firewall that matched the rule. The circled number next to Apps Seen indicates how many applications were seen on the rule. • **Applications**—The applications seen on the rule. For example, if a rule allows web-browsing traffic (Apps on Rule), you may see many applications in the list because there are many web-browsing applications. • **Subcategory**—The subcategory of the application. • **Risk**—The risk rating of the application.

Field	Description
	• **First Seen**—The first day the application was seen on the network. • **Last Seen**—The most recent day the application was seen on the network.  *The granularity of measurement for First Seen and Last Seen is one day, so on the day you define a rule, the First Day and Last Day are the same day.* • **Traffic (30 days)**—The amount of traffic in bytes seen during the last 30-day period.  *A longer time period would result in the oldest rules remaining at the top of the list because they are likely to have the most cumulative traffic. This can result in newer rules being listed below older rules even if the newer rules see heavy traffic.*
Apps Seen Actions	Actions you can perform on **Apps Seen**: • **Create Cloned Rule**—Clones the current rule. When migrating from port-based rules to application-based rules, clone the port-based rule first and then edit the clone to create the application-based rule that allows the traffic. The cloned rule is inserted above the port-based rule in the policy list. Use this migration method to ensure that you don't inadvertently deny traffic that you want to allow—if the cloned rule doesn't allow all the applications you need, the port-based rule that follows allows them. Monitor the port-based rule and adjust the (cloned) application-based rule as needed. When you're sure the application-based rule allows the traffic you want and only unwanted traffic filters through to the port-based rule, you can safely remove the port-based rule. • **Add to This Rule**—Adds applications from Apps Seen to the rule. Adding applications to the rule transforms a rule configured to match **Any** application (a port-based rule) to an application-based rule that allows the applications you specify (the new application-based rule replaces the port-based rule). The rule denies any applications that you don't add just as with any other application-based rule. Be sure to identify all applications you want to allow and add them to the rule so you don't accidentally deny an application. • **Add to Existing Rule**—Adds applications from Apps Seen to an existing application-based (App-ID) rule. This enables you to clone an App-ID-based rule from a port-based rule, then add more applications seen on port-based rules to the App-ID rule later. • **Match Usage**—Moves all Apps Seen into the rule (they are listed under Apps on Rule after you **Match Usage**). If you are certain that the rule should allow *all* listed applications, **Match Usage** is very convenient. However, you must be certain that all listed applications are applications you want to allow on

Field	Description
	your network. If many applications have been seen on the rule (for example, on a rule that allows web-browsing), it's better to clone the rule and transition to an application-based rule. **Match Usage** works well for simple rules with well-known applications. For example, if a port-based rule for port 22 has only seen SSH traffic (and that's all it should see), it's safe to **Match Usage**.
Clone dialog Add to This Rule dialog Add Apps to Existing Rule dialog	When you select applications from **Apps Seen** and **Create Cloned Rule** or **Add to Rule** that have related applications, these dialogs list: • **Name** (Clone and Add Apps to Existing Rule dialogs only). • Clone: Enter the name of the new cloned rule. • Add Apps to Existing Rule: Select the rule to which to add applications from the drop-down menu or enter the name of the rule. • **Applications**: • Add container app (default): Selects the checkboxes of all the container apps, the apps seen on the rule, and the apps in the container that have not been seen on the rule. • Add specific apps seen: Selects only the apps that have actually been seen on the rule and deselects everything else. (You can manually select container apps and other apps.) • **Application**: • The selected applications that were seen on the rule, highlighted green. • Container apps, highlighted gray, with their individual applications listed below. • Individual applications in a container that have been seen on the rule but were not selected in **Applications & Usage**(normal text). • Individual applications in a container that have not been seen on the rule (*italics*). • The date applications were **Last Seen** on the rule. • **Dependent Applications**: • The checkbox for adding application dependencies is checked by default because these applications are required for the selected application to run. • **Depends On**—The list of dependent applications for the selected applications. The applications you selected require these dependent applications to run. • **Required By**—Lists the application that requires the dependent application (**Depends On**). (Sometimes a dependent application in turn requires another dependent application.) The **Clone**, **Add to Rule**, and **Add Apps to Existing Rule** dialogs help to ensure that applications don't break and enable you to

Field	Description
	future-proof the rule by including relevant individual applications that are related to the applications you're cloning or adding to a rule.

Security Policy Optimizer

- Policies > Security > Policy Optimizer

Policies > **Security** > **Policy Optimizer** displays:

- **No App Specified**—Rules that have the application set to **any**, so you can identify port-based rules to convert to application-based rules.
- **Unused Apps**—Rules that include applications that have never matched the rule.
- **Rule Usage**—Rule usage information over different periods of time, including rules not used over different periods of time.

Field	Description
Name	The name of the Security policy rule.
Service	Any services associated with the Security policy rule.
Traffic (Bytes, 30 days)	**Traffic (30 days)**—The amount of traffic in bytes seen during the last 30-day period.  *A longer time period would result in the oldest rules remaining at the top of the list because they are likely to have the most cumulative traffic. This can result in newer rules being listed below older rules even if the newer rules see heavy traffic.*
Apps Allowed	The applications that the rule allows. Open the **Application** dialog, from which you can add and delete applications on the rule.
Apps Seen	The number of applications seen on the rule. Click the number to open the **Applications & Usage** dialog, which enables you to compare the applications configured on the rule against the applications seen on the rule and to modify the applications.
Day with No New Apps	The number of days since the last new application was seen on the rule.
Compare	Opens the **Applications & Usage** dialog to compare the applications configured on the rule against the applications seen on the rule and modify the rule.
(Rule Usage) Last Hit	The most recent time that traffic matched the rule.
(Rule Usage) First Hit	The first time that traffic matched the rule.

Field	Description
(Rule Usage) Hit Count	The number of times that traffic matched the rule.
Modified	The date and time that the rule was last modified.
Created	The date and time that the rule was created.
Timeframe (Rule Usage only)	The time period (number of days) for which data is displayed.
Usage (Rule Usage only)	Displays: • **Any** (all) rules on the firewall over the specified Timeframe, regardless of whether traffic matched the rules (used rules) or not (unused rules). • **Unused** rules that traffic has not matched over the specified Timeframe. • **Used** rules that traffic has matched over the specified Timeframe.
Exclude rules reset during the last *xx* days (Rule Usage only)	Does not display rules for which you **Reset Rule Hit Counter** within the specified number of days (from 1-5,000 days). For example, this enables you to examine older rules that have not matched traffic over a Timeframe while excluding newer rules that may not have had time to match traffic.
Reset Date (Rule Usage only)	The last date on which the rule's hit counter was reset.

Policies > NAT

If you define Layer 3 interfaces on the firewall, you can configure a Network Address Translation (NAT) policy to specify whether source or destination IP addresses and ports are converted between public and private addresses and ports. For example, private source addresses can be translated to public addresses on traffic sent from an internal (trusted) zone to a public (untrusted) zone. NAT is also supported on virtual wire interfaces.

NAT rules are based on source and destination zones, source and destination addresses, and application service (such as HTTP). Like security policies, NAT policy rules are compared against incoming traffic in sequence, and the first rule that matches the traffic is applied.

As needed, add static routes to the local router so that traffic to all public addresses is routed to the firewall. You may also need to add static routes to the receiving interface on the firewall to route traffic back to the private address.

The following tables describe the NAT and NPTv6 (IPv6-to-IPv6 Network Prefix Translation) settings:

- NAT Policies General Tab
- NAT Original Packet Tab
- NAT Translated Packet Tab
- NAT Active/Active HA Binding Tab
- (Panorama only) NAT Target Tab

Looking for more?

See NAT

NAT Policies General Tab

- **Policies** > **NAT** > **General**

Select the **General** tab to configure a name and description for the NAT or NPTv6 policy. You can configure a tag to allow you to sort or filter policies when many policies exist. Select the type of NAT policy you are creating, which affects which fields are available on the **Original Packet** and **Translated Packet** tabs.

NAT Rule - General Settings	Description
Name	Enter a name to identify the rule. The name is case-sensitive and can have up to 63 characters, which can be letters, numbers, spaces, hyphens, and underscores. The name must be unique on a firewall and, on Panorama, unique within its device group and any ancestor or descendant device groups.
Description	Enter a description for the rule (up to 1024 characters).
Tag	If you want to tag the policy, **Add** and specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword.
Group Rules by Tag	Enter a tag with which to group similar policy rules. The group tag allows you to view your policy rule base based on these tags. You can group rules based on a **Tag**.

NAT Rule - General Settings	Description
NAT Type	Specify the type of translation: • **ipv4**—translation between IPv4 addresses. • **nat64**—translation between IPv6 and IPv4 addresses. • **nptv6**—translation between IPv6 prefixes. You cannot combine IPv4 and IPv6 address ranges in a single NAT rule.
Audit Comment	Enter a comment to audit the creation or editing of the policy rule. The audit comment is case-sensitive and can have up to 256 characters, which can be letters, numbers, spaces, hyphens, and underscores.
Audit Comment Archive	View previous **Audit Comments** for the policy rule. You can export the Audit Comment Archive CSV format.

NAT Original Packet Tab

- Policies > NAT > Original Packet

Select the **Original Packet** tab to define the source and destination zones of packets that the firewall will translate and, optionally, specify the destination interface and type of service. You can configure multiple source and destination zones of the same type and you can apply the rule to specific networks or specific IP addresses.

NAT Rule - Original Packet Settings	Description
Source Zone / Destination Zone	Select one or more source and destination zones for the original (non-NAT) packet (default is **Any**). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones. You can specify multiple zones to simplify management. For example, you can configure settings so that multiple internal NAT addresses are directed to the same external IP address.
Destination Interface	Specify the destination interface of packets the firewall translates. You can use the destination interface to translate IP addresses differently in the case where the network is connected to two ISPs with different IP address pools.
Service	Specify the service for which the firewall translates the source or destination address. To define a new service group, select Objects > Service Groups.
Source Address / Destination Address	Specify a combination of source and destination addresses for the firewall to translate. For NPTv6, the prefixes configured for **Source Address** and **Destination Address** must be in the format xxxx:xxxx::/yy. The address cannot have an interface identifier (host) portion defined. The range of supported prefix lengths is /32 to /64.

NAT Translated Packet Tab

- Policy > NAT > Translated Packet

For Source Address Translation, select the **Translated Packet** tab to determine the type of translation to perform on the source, the address, and possibly the port to which the source is translated.

You can also enable Destination Address Translation for an internal host to make it accessible by a public IP address. In this case, you define a public source address and destination address in the **Original Packet** tab for an internal host and, on the **Translated Packet** tab, you configure **Static IP** or **Dynamic IP (with session distribution)** and enter the **Translated Address**. Then, when the public address is accessed, it is translated to the internal (destination) address of the internal host.

NAT Rule - Translated Packet Settings	Description
Source Address Translation	Select the **Translation Type** (dynamic or static address pool) and enter an IP address or address range (address1—address2) to which the source address is translated (**Translated Address**). The size of the address range is limited by the type of address pool: • **Dynamic IP and Port**—Address selection is based on a hash of the source IP address. For a given source IP address, the firewall uses the same translated source address for all sessions. Dynamic IP and Port (DIPP) source NAT supports approximately 64,000 concurrent sessions on each IP address in the NAT pool. Some models support oversubscription, which allows a single IP to host more than 64,000 concurrent sessions. Palo Alto Networks® DIPP NAT supports more NAT sessions than are supported by the number of available IP addresses and ports. With oversubscription, the firewall can use IP address and port combinations two times simultaneously on PA-220, PA-820, PA-850, VM-50, VM-300, and VM-1000-HV firewalls, four times simultaneously on PA-5220 firewall and PA-3200 Series firewalls, and eight times simultaneously on PA-5250, PA-5260, PA-5280, PA-7050, PA-7080, VM-500, and VM-700 firewalls when destination IP addresses are unique. • **Dynamic IP**—Translates to the next available address in the specified range but the port number remains unchanged. Up to 32,000 consecutive IP addresses are supported. A dynamic IP pool can contain multiple subnets, so you can translate your internal network addresses to two or more separate public subnets. • **Advanced (Dynamic IP/Port Fallback)**—Use this option to create a fallback pool that performs IP and port translation and is used if the primary pool runs out of addresses. You can define addresses for the pool by using the **Translated Address** option or the **Interface Address** option; the latter option is for interfaces that receive an IP address dynamically. When creating a fallback pool, make sure addresses do not overlap with addresses in the primary pool.
Source Address Translation (cont)	• **Static IP**—The same address is always used for the translation and the port is unchanged. For example, if the source range is 192.168.0.1—192.168.0.10 and the translation range is 10.0.0.1—10.0.0.10, address 192.168.0.2 is always translated to 10.0.0.2. The address range is virtually unlimited. You must use **Static IP** translation for NPTv6 Source Address Translation. For NPTv6, the prefixes configured for **Translated Address** must be in the format xxxx:xxxx::/yy and the address cannot have an interface identifier (host) portion defined. The range of supported prefix lengths is /32 to /64.

NAT Rule - Translated Packet Settings	Description
	• **None**—Translation is not performed.
Bi-directional	(Optional) Enable bidirectional translation for a **Static IP** source address translation if you want the firewall to create a corresponding translation (NAT or NPTv6) in the opposite direction of the translation you configure. *If you enable bidirectional translation, you must ensure that you have security policies in place to control the traffic in both directions. Without such policies, the bidirectional feature allows packets to be translated automatically in both directions.*
Destination Address Translation	Configure the following options to have the firewall perform destination NAT. You typically use Destination NAT to allow an internal server, such as an email server, to be accessible from the public network.
Translation Type and Translated Address	Select the type of translation the firewall performs on the destination address: • **None** (default) • **Static IP**—Enter a **Translated Address** as an IP address or range of IP addresses and a **Translated Port** number (1 to 65535) to which the original destination address and port number are translated. If the **Translated Port** field is blank, the destination port is not changed. For NPTv6, the prefixes configured for the Destination prefix **Translated Address** must be in the format xxxx:xxxx::/yy. The address cannot have an interface identifier (host) portion defined. The range of supported prefix lengths is /32 to /64. *Translated Port is not supported for NPTv6 because NPTv6 is strictly prefix translation. The Port and Host address section is simply forwarded unchanged.* *Static IP translation for IPv4 also allows you to Enable DNS Rewrite (described below).* • **Dynamic IP (with session distribution)**—Select or enter a **Translated Address** that is an FQDN, an address object, or an address group from which the firewall selects the translated address. If the DNS server returns more than one address for an FQDN or if the address object or address group translates into more than one IP address, the firewall distributes sessions among those addresses using the specified **Session Distribution Method**.
Session Distribution Method	If you select the destination NAT translation to be to **Dynamic IP (with session distribution)**, it's possible that the destination translated address (to an FQDN, address object, or address group) can resolve to more than one address. You can choose how the firewall distributes (assigns) sessions among those addresses to provide more balanced session distribution: • **Round Robin**—(default) Assigns new sessions to IP addresses in rotating order. Unless your environment dictates that you choose one of the other distribution methods, use this method.

NAT Rule - Translated Packet Settings	Description
	• **Source IP Hash**—Assigns new sessions based on a hash of source IP addresses. If you have incoming traffic from a single source IP address, then select a method other than **Source IP Hash**. • **IP Modulo**—The firewall takes into consideration the source and destination IP address from the incoming packet; the firewall performs an XOR operation and a modulo operation; the result determines to which IP address the firewall assigns new sessions. • **IP Hash**—Assigns new sessions using a hash of the source and destination IP addresses. • **Least Sessions**—Assigns new sessions to the IP address that has the fewest concurrent sessions. If you have many short-lived sessions, **Least Sessions** provides you with a more balanced distribution of sessions.
Enable DNS Rewrite	In PAN-OS 9.0.2 and later 9.0 releases, if the destination NAT policy rule type is **ipv4** and the destination address translation type is **Static IP**, the **Enable DNS Rewrite** option is available. You can enable DNS rewrite if you use destination NAT and also use DNS services on one side of the firewall to resolve FQDNs for a client on the other side of the firewall. When the DNS response traverses the firewall, the firewall rewrites the IP address in the DNS response, relative to the original destination address or translated destination address that the DNS response matches in the NAT policy rule. A single NAT policy rule has the firewall perform NAT on packets that match the rule and perform NAT on IP addresses in DNS responses that match the rule. You must specify how the firewall performs NAT on an IP address in a DNS response relative to the NAT rule—reverse or forward: • **reverse**—(default) If the packet is a DNS response that matches the translated destination address in the rule, translate the DNS response using the reverse translation that the rule uses. For example, if the rule translates 1.1.1.10 to 192.168.1.10, the firewall rewrites a DNS response of 192.168.1.10 to 1.1.1.10. • **forward**—If the packet is a DNS response that matches the original destination address in the rule, translate the DNS response using the same translation the rule uses. For example, if the rule translates 1.1.1.10 to 192.168.1.10, the firewall rewrites a DNS response of 1.1.1.10 to 192.168.1.10.

NAT Active/Active HA Binding Tab

- Policies > NAT > Active/Active HA Binding

The Active/Active HA Binding tab is available only if the firewall is in a high availability (HA) active/active configuration. In this configuration, you must bind each source NAT rule (whether static or dynamic NAT) to Device ID 0 or Device ID 1; you must bind each destination NAT rule to either Device ID **0**, Device ID **1**, **both** (Device ID 0 and Device ID 1), or to the active-**primary** firewall.

Select an **Active/Active HA Binding** setting to bind the NAT rule to an HA firewall as follows:

- **0**—Binds the NAT rule to the firewall that has HA Device ID 0.
- **1**—Binds the NAT rule to the firewall that has HA Device ID 1.
- **both**—Binds the NAT rule to both the firewall that has HA Device ID 0 and the firewall that has HA Device ID 1. This setting does not support Dynamic IP or Dynamic IP and Port NAT.
- **primary**—Binds the NAT rule to the firewall that is in HA active-primary state. This setting does not support Dynamic IP or Dynamic IP and Port NAT.

You typically configure device-specific NAT rules when the two HA peers have unique NAT IP address pools.

When the firewall creates a new session, the HA binding determines which NAT rules the session can match. The binding must include the session owner for the rule to match. The session setup firewall performs the NAT rule matching but the session is compared to NAT rules that are bound to the session owner and translated according to one of the rules. For device-specific rules, the firewall skips all NAT rules that are not bound to the session owner. For example, suppose the firewall with Device ID 1 is the session owner and the session setup firewall. When Device ID 1 attempts to match a session to a NAT rule, it ignores all rules bound to Device ID 0.

If one peer fails, the second peer continues to process traffic for the synchronized sessions from the failed peer, including NAT translations. Palo Alto Networks recommends you create a duplicate NAT rule that is bound to the second Device ID. Therefore, there are two NAT rules with the same source translation addresses and the same destination translation addresses—one rule bound to each Device ID. This configuration allows the HA peer to perform new session setup tasks and perform NAT rule matching for NAT rules that are bound to its Device ID. Without a duplicate NAT rule, the functioning peer will try to perform the NAT policy match but the session won't match the firewall's own device-specific rules and the firewall skips all other NAT rules that are not bound to its Device ID.

Looking for more?

See NAT in Active/Active HA Mode

NAT Target Tab

- (Panorama only) **Policies** > **NAT** > **Target**

Select the **Target** tab to select which managed firewalls in the device group to push the policy rule to. You can specify which managed firewalls to push to by select the managed firewalls or by specifying a tag. Additionally, you can configure the policy rule target to push to all managed firewalls except for those specified.

NAT Rule - Target Settings	Description
Any (target all devices)	Enable (check) to push the policy rule to all managed firewalls in the device group.
Devices	Select one or more managed firewalls associated with the device group to push the policy rule to.
Tags	**Add** one or more tags to push the policy rule to managed firewalls in the device group with the specified tag.
Target to all but these specified devices and tags	Enable (check) to push the policy rule to all managed firewalls associated with the device group except for the selected device(s) and tag(s).

Policies > QoS

Add QoS policy rules to define the traffic that receives specific QoS treatment and assign a QoS class for each QoS policy rule to specify that the assigned class of service applies to all traffic matched to the associated rule as it exits a QoS-enabled interface.

QoS policy rules pushed to a firewall from Panorama are shown in orange and cannot be edited at the firewall level.

Additionally, to fully enable the firewall to provide QoS:

- Set bandwidth limits for each QoS class of service (select Network > Network Profiles > QoS to add or modify a QoS profile).
- Enable QoS on an interface (select Network > QoS).

Refer to Quality of Service for complete QoS workflows, concepts, and use cases.

Add a new rule or clone an existing rule and then define the following fields.

QoS Policy Rule Settings	
General Tab	
Name	Enter a name to identify the rule (up to 63 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter an optional description.
Tag	If you need to tag the policy, **Add** and specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.
Group Rules by Tag	Enter a tag with which to group similar policy rules. The group tag allows you to view your policy rule base based on these tags. You can group rules based on a **Tag**.
Audit Comment	Enter a comment to audit the creation or editing of the policy rule. The audit comment is case-sensitive and can have up to 256 characters, which can be letters, numbers, spaces, hyphens, and underscores.
Audit Comment Archive	View previous **Audit Comments** for the policy rule. You can export the Audit Comment Archive in CSV format.
Source Tab	
Source Zone	Select one or more source zones (default is **any**). Zones must be of the same type (Layer 2, Layer 3, or virtual wire).

QoS Policy Rule Settings	
Source Address	Specify a combination of source IPv4 or IPv6 addresses for which the identified application can be overridden. To select specific addresses, choose **select** from the drop-down and do any of the following: • Select this option next to the appropriate addresses  and/or address groups  in the Available column, and click **Add** to add your selections to the Selected column. • Enter the first few characters of a name in the search field to list all addresses and address groups that start with those characters. Selecting an item in the list enables this option in the Available column. Repeat this process as often as needed, and then click **Add**. • Enter one or more IP addresses (one per line), with or without a network mask. The general format is: *<ip_address>/<mask>* • To remove addresses, select them (Selected column) and click **Delete** or select **any** to clear all addresses and address groups. To add new addresses that can be used in this or other policies, click **New Address**. To define new address groups, select Objects > Address Groups.
Source User	Specify the source users and groups to which the QoS policy will apply.
Negate	Select this option to have the policy apply if the specified information on this tab does NOT match.
Destination Tab	
Destination Zone	Select one or more destination zones (default is **any**). Zones must be of the same type (Layer 2, Layer 3, or virtual wire).
Destination Address	Specify a combination of source IPv4 or IPv6 addresses for which the identified application can be overridden. To select specific addresses, choose **select** from the drop-down and do any of the following: • Select this option next to the appropriate addresses  and/or address groups  in the Available column, and **Add** your selections to the Selected column. • Enter the first few characters of a name in the search field to list all addresses and address groups that start with those characters. Selecting an item in the list enables this option in the Available column. Repeat this process as often as needed, and then click **Add**. • Enter one or more IP addresses (one per line), with or without a network mask. The general format is: *<ip_address>/<mask>*. • To remove addresses, select them (Selected column) and click **Delete** or select **any** to clear all addresses and address groups. To add new addresses that can be used in this or other policies, click **New Address**.
Negate	Select this option to have the policy apply if the specified information on this tab does not match.

QoS Policy Rule Settings	
Application Tab	
Application	Select specific applications for the QoS rule. To define new applications or application groups, select **Objects** > **Applications**. If an application has multiple functions, you can select the overall application or individual functions. If you select the overall application, all functions are included, and the application definition is automatically updated as future functions are added. If you are using application groups, filters, or container in the QoS rule, you can view details on these objects by holding your mouse over the object in the Application column, click the down arrow and select **Value**. This enables you to easily view application members directly from the policy without having to go to the **Objects** tab.
Service/URL Category Tab	
Service	Select services to limit to specific TCP and/or UDP port numbers. Choose one of the following from the drop-down: • **any**—The selected applications are allowed or denied on any protocol or port. • **application-default**—The selected applications are allowed or denied only on their default **ports defined by Palo Alto Networks**. This option is recommended for allow policies. • **Select**—Click **Add**. Choose an existing service or choose **Service** or **Service Group** to specify a new entry.
URL Category	Select URL categories for the QoS rule. • Select **Any** to ensure that a session can match this QoS rule regardless of the URL category. • To specify a category, click **Add** and select a specific category (including a custom category) from the drop-down. You can add multiple categories. Refer to Objects > External Dynamic Lists for information on defining custom categories.
DSCP/TOS Tab	
Any	Select **Any** (default) to allow the policy to match to traffic regardless of the Differentiated Services Code Point (DSCP) value or the IP Precedence/Type of Service (ToS) defined for the traffic.
Codepoints	Select **Codepoints** to enable traffic to receive QoS treatment based on the DSCP or ToS value defined a packet's IP header. The DSCP and ToS values are used to indicate the level of service requested for traffic, such as high priority or best effort delivery. Using codepoints as matching criteria in a QoS policy allows a session to receive QoS treatment based on the codepoint detected at the beginning of the session. Continue to **Add** codepoints to match traffic to the QoS policy: • Give codepoint entries a descriptive **Name**.

QoS Policy Rule Settings	
	• Select the **Type** of codepoint you want to use as matching criteria for the QoS policy and then select a specific **Codepoint** value. You can also create a **Custom Codepoint** by entering a **Codepoint Name** and **Binary Value**.
Other Settings Tab	
Class	Choose the QoS class to assign to the rule, and click **OK**. Class characteristics are defined in the QoS profile. Refer to Network > Network Profiles > QoS for information on configuring settings for QoS classes.
Schedule	• Select **None** for the policy rule to remain active at all times. • From the drop-down, select **Schedule** (calendar icon) to set a single time range or a recurring time range during which the rule is active.
Target Tab (Panorama only)	
Any (target all devices)	Enable (check) to push the policy rule to all managed firewalls in the device group.
Devices	Select one or more managed firewalls associated with the device group to push the policy rule to.
Tags	**Add** one or more tags to push the policy rule to managed firewalls in the device group with the specified tag.
Target to all but these specified devices and tags	Enable (check) to push the policy rule to all managed firewalls associated with the device group except for the selected device(s) and tag(s).

Policies > Policy Based Forwarding

Normally, when traffic enters the firewall, the ingress interface virtual router dictates the route that determines the outgoing interface and destination security zone based on destination IP address. By creating a policy-based forwarding (PBF) rule, you can specify other information to determine the outgoing interface, including source zone, source address, source user, destination address, destination application, and destination service. The initial session on a given destination IP address and port that is associated with an application will not match an application-specific rule and will be forwarded according to subsequent PBF rules (that do not specify an application) or the virtual router's forwarding table. All subsequent sessions on that destination IP address and port for the same application will match an application-specific rule. To ensure forwarding through PBF rules, application-specific rules are not recommended.

When necessary, PBF rules can be used to force traffic through an additional virtual system using the Forward-to-VSYS forwarding action. In this case, it is necessary to define an additional PBF rule that will forward the packet from the destination virtual system out through a particular egress interface on the firewall.

The following tables describe the policy-based forwarding settings:

- Policy Based Forwarding General Tab
- Policy Based Forwarding Source Tab
- Policy Based Forwarding Destination/Application/Service Tab
- Policy Based Forwarding Forwarding Tab
- (Panorama only) Policy Based Forwarding Target Tab

Looking for more?

Refer to Policy-Based Forwarding

Policy Based Forwarding General Tab

Select the **General** tab to configure a name and description for the PBF policy. A tag can also be configured to allow you to sort or filter policies when a large number of policies exist.

Field	Description
Name	Enter a name to identify the rule. The name is case-sensitive and can have up to 63 characters, which can be letters, numbers, spaces, hyphens, and underscores. The name must be unique on a firewall and, on Panorama, unique within its device group and any ancestor or descendant device groups.
Description	Enter a description for the policy (up to 1024 characters).
Tag	If you need to tag the policy, **Add** and specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.

Field	Description
Group Rules by Tag	Enter a tag with which to group similar policy rules. The group tag allows you to view your policy rule base based on these tags. You can group rules based on a **Tag**.
Audit Comment	Enter a comment to audit the creation or editing of the policy rule. The audit comment is case-sensitive and can have up to 256 characters, which can be letters, numbers, spaces, hyphens, and underscores.
Audit Comment Archive	View previous **Audit Comments** for the policy rule. You can export the Audit Comment Archive in CSV format.

Policy Based Forwarding Source Tab

Select the **Source** tab to define the source zone or source address that defines the incoming source traffic to which the forwarding policy will be applied.

Field	Description
Source Zone	To choose source zones (default is any), click **Add** and select from the drop-down. To define new zones, refer to Network > Zones. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases. *Only Layer 3 type zones are supported for policy-based forwarding.*
Source Address	Click **Add** to add source addresses, address groups, or regions (default is any). Select from the drop-down, or click **Address**, **Address Group**, or **Regions** at the bottom of the drop-down, and specify the settings.
Source User	Click **Add** to choose the source users or groups of users subject to the policy. The following source user types are supported: • **any**—Include any traffic regardless of user data. • **pre-logon**—Include remote users that are connected to the network using GlobalProtect™, but are not logged into their system. When the Pre-logon option is configured on the Portal for GlobalProtect apps, any user who is not currently logged into their machine will be identified with the username pre-logon. You can then create policies for pre-logon users and although the user is not logged in directly, their machines are authenticated on the domain as if they were fully logged in. • **known-user**—Includes all authenticated users, which means any IP with user data mapped. This option is equivalent to the “domain users” group on a domain. • **unknown**—Includes all unauthenticated users, which means IP addresses that are not mapped to a user. For example, you could use unknown for guest level access to something because they will have an IP on your

Field	Description
	network, but will not be authenticated to the domain and will not have IP address-to-user mapping information on the firewall. • **Select**—Includes selected users as determined by the selection in this window. For example, you may want to add one user, a list of individuals, some groups, or manually add users.  *If the firewall collects user information from a RADIUS, TACACS+, or SAML identity provider server and not from the User-ID™ agent, the list of users does not display; you must enter user information manually.*

Policy Based Forwarding Destination/Application/Service Tab

Select the **Destination/Application/Service** tab to define the destination settings that will be applied to traffic that matches the forwarding rule.

Field	Description
Destination Address	Click **Add** to add destination addresses or address groups (default is any). By default, the rule applies to **Any** IP address. Select from the drop-down, or click **Address** or **Address Group** at the bottom of the drop-down, and specify the settings.
Application/Service	Select specific applications or services for the PBF rule. To define new applications, refer to Defining Applications. To define application groups, refer to Objects > Application Groups.  *Application-specific rules are not recommended for use with PBF. Whenever possible, use a service object, which is the Layer 4 port (TCP or UDP) used by the protocol or application.* You can view details on these applications by holding your mouse over the object in the **Application** column, clicking the down arrow, and selecting **Value**. This enables you to easily view application information directly from the policy without having to go to the Object tabs.  *You cannot use custom applications, application filters, or application groups in PBF rules.*

Policy Based Forwarding Forwarding Tab

Select the **Forwarding** tab to define the action and network information that will be applied to traffic that matches the forwarding policy. Traffic can be forwarded to a next-hop IP address, a virtual system, or the traffic can be dropped.

Field	Description
Action	Select one of the following options: • **Forward**—Specify the next hop IP address and egress interface (the interface that the packet takes to get to the specified next hop). • **Forward To VSYS**—Choose the virtual system to forward to from the drop-down. • **Discard**—Drop the packet. • **No PBF**—Do not alter the path that the packet will take. This option, excludes the packets that match the criteria for source/destination/ application/service defined in the rule. Matching packets use the route table instead of PBF; the firewall uses the route table to exclude the matched traffic from the redirected port.  *Use Forward or Forward to VSYS as the Action so you can apply a Monitor profile to the traffic. (You can't apply a Monitor profile when the Action doesn't forward the traffic.) Monitor profiles monitor the IP address. If connectivity to the IP address fails, Monitor profiles specify the action.*
Egress Interface	Directs the packet to a specific Egress Interface
Next Hop	If you direct the packet to a specific interface, specify the Next Hop for the packet in one of the following ways: • **IP Address**—Select IP Address and select an address object (or create a new address object) that uses an IPv4 or IPv6 address. • **FQDN**—Select FQDN and select an address object (or create a new address object) that uses an FQDN. • **None**—There is no next hop; the packet is dropped.
Monitor	Enable Monitoring to verify connectivity to a target **IP Address** or to the **Next Hop** IP address. Select **Monitor** and attach a monitoring **Profile** (default or custom, **Network** > **Network Profiles** > **Monitor**) that specifies the action when the IP address is unreachable.  *Configure Monitor profiles and enable monitoring so that if the egress interface fails or the route goes down, the firewall takes the action in the profile and minimizes or prevents the service interruption.*
Enforce Symmetric Return	(Required for asymmetric routing environments) Select **Enforce Symmetric Return** and enter one or more IP addresses in the **Next Hop Address** List. Enabling symmetric return ensures that return traffic (such as from the Trust zone on the LAN to the Internet) is forwarded out through the same interface through which traffic ingresses from the internet.
Schedule	To limit the days and times when the rule is in effect, select a schedule from the drop-down. To define new schedules, refer to Settings to Control Decrypted SSL Traffic.

Policy Based Forwarding Target Tab

- (Panorama only) **Policies** > **Policy Based Forwarding** > **Target**

Select the **Target** tab to select which managed firewalls in the device group to push the policy rule to. You can specify which managed firewalls to push to by select the managed firewalls or by specifying a tag. Additionally, you can configure the policy rule target to push to all managed firewalls except for those specified.

NAT Rule - Target Settings	Description
Any (target all devices)	Enable (check) to push the policy rule to all managed firewalls in the device group.
Devices	Select one or more managed firewalls associated with the device group to push the policy rule to.
Tags	**Add** one or more tags to push the policy rule to managed firewalls in the device group with the specified tag.
Target to all but these specified devices and tags	Enable (check) to push the policy rule to all managed firewalls associated with the device group except for the selected device(s) and tag(s).

Policies > Decryption

You can configure the firewall to decrypt traffic for visibility, control, and granular security. Decryption policies can apply to Secure Sockets Layer (SSL) including SSL encapsulated protocols such as IMAP(S), POP3(S), SMTP(S), and FTP(S), and Secure Shell (SSH) traffic. SSH decryption can be used to decrypt outbound and inbound SSH traffic to assure that secure protocols are not being used to tunnel disallowed applications and content.

Add a decryption policy rule to define traffic that you want to decrypt (for example, you can decrypt traffic based on URL categorization). Decryption policy rules are compared against the traffic in sequence, so more specific rules must precede the more general ones.

SSL forward proxy decryption requires the configuration of a trusted certificate that is presented to the user if the server to which the user is connecting possesses a certificate signed by a CA trusted by the firewall. Create a certificate on the **Device** > **Certificate Management** > **Certificates** page and then click the name of the certificate and select **Forward Trust Certificate**.

The firewall doesn't decrypt applications that break decryption technically, for example because they use pinned certificates or client authentication.

Refer to the List of Applications Excluded from SSL Decryption*.*

The following tables describe the decryption policy settings:

- Decryption General Tab
- Decryption Source Tab
- Decryption Destination Tab
- Decryption Service/URL Category Tab
- Decryption Options Tab
- (Panorama only) Decryption Target Tab

Looking for more?

See Decryption

Decryption General Tab

Select the **General** tab to configure a name and description for the decryption policy. You can also configure a tag to allow you to sort or filter policies when a large number of policies exist.

Field	Description
Name	Enter a name to identify the rule. The name is case-sensitive and can have up to 63 characters, which can be letters, numbers, spaces, hyphens, and underscores. The name must be unique on a firewall and, on Panorama, unique within its device group and any ancestor or descendant device groups.
Description	Enter a description for the rule (up to 1024 characters).
Tag	If you need to tag the policy, **Add** and specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want

Field	Description
	to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.
Group Rules by Tag	Enter a tag with which to group similar policy rules. The group tag allows you to view your policy rule base based on these tags. You can group rules based on a **Tag**.
Audit Comment	Enter a comment to audit the creation or editing of the policy rule. The audit comment is case-sensitive and can have up to 256 characters, which can be letters, numbers, spaces, hyphens, and underscores.
Audit Comment Archive	View previous **Audit Comments** for the policy rule. You can export the Audit Comment Archive in CSV format.

Decryption Source Tab

Select the **Source** tab to define the source zone or source address that defines the incoming source traffic to which the decryption policy will be applied.

Field	Description
Source Zone	Click **Add** to choose source zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.
Source Address	Click **Add** to add source addresses, address groups, or regions (default is any). Select from the drop-down, or click **Address**, **Address Group**, or **Regions** at the bottom of the drop-down, and specify the settings. Select **Negate** to choose any address except the configured ones.
Source User	Click **Add** to choose the source users or groups of users subject to the policy. The following source user types are supported: • **any**—Include any traffic regardless of user data. • **pre-logon**—Include remote users that are connected to the network using GlobalProtect, but are not logged into their system. When the Pre-logon option is configured on the Portal for GlobalProtect apps, any user who is not currently logged into their machine will be identified with the username pre-logon. You can then create policies for pre-logon users and although the user is not logged in directly, their machines are authenticated on the domain as if they were fully logged in. • **known-user**—Includes all authenticated users, which means any IP with user data mapped. This option is equivalent to the “domain users” group on a domain.

Field	Description
	• **unknown**—Includes all unauthenticated users, which means IP addresses that are not mapped to a user. For example, you could use unknown for guest level access to something because they will have an IP on your network, but will not be authenticated to the domain and will not have IP to user mapping information on the firewall. • **Select**—Includes selected users as determined by the selection in this window. For example, you may want to add one user, a list of individuals, some groups, or manually add users. *If the firewall collects user information from a RADIUS, TACACS+, or SAML identity provider server and not from the User-ID™ agent, the list of users does not display; you must enter user information manually.*

Decryption Destination Tab

Select the **Destination** tab to define the destination zone or destination address that defines the destination traffic to which the policy will be applied.

Field	Description
Destination Zone	Click **Add** to choose destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.
Destination Address	Click **Add** to add destination addresses, address groups, or regions (default is any). Select from the drop-down, or click **Address**, **Address Group**, or **Regions** at the bottom of the drop-down, and specify the settings. Select **Negate** to choose any address except the configured ones.

Decryption Service/URL Category Tab

Select the **Service/URL Category** tab to apply the decryption policy to traffic based on TCP port number or to any URL category (or a list of categories).

Field	Description
Service	Apply the decryption policy to traffic based on specific TCP port numbers. Choose one of the following from the drop-down: • **any**—The selected applications are allowed or denied on any protocol or port.

Field	Description
	• **application-default**—The selected applications are decrypted (or are exempt from decryption) only on the default ports defined for the applications by Palo Alto Networks. • **Select**—Click **Add**. Choose an existing service or specify a new **Service** or **Service Group**. (Or select Objects > Services and Objects > Service Groups).
URL Category Tab	Select URL categories for the decryption rule. • Choose **any** to match any sessions regardless of the URL category. • To specify a category, click **Add** and select a specific category (including a custom category) from the drop-down. You can add multiple categories. Refer to for information on defining custom categories.

Decryption Options Tab

Select the **Options** tab to determine if the matched traffic should be decrypted or not. If **Decrypt** is set, specify the decryption type. You can also add additional decryption features by configuring or selecting a decryption profile.

Field	Description
Action	Select **decrypt** or **no-decrypt** for the traffic.
Type	Select the type of traffic to decrypt from the drop-down: • **SSL Forward Proxy**—Specifies that the policy will decrypt client traffic destined for an external server. • **SSH Proxy**—Specifies that the policy will decrypt SSH traffic. This option allows you to control SSH tunneling in policies by specifying the ssh-tunnel App-ID. • **SSL Inbound Inspection**—Specifies that the policy will decrypt SSL inbound inspection traffic.
Decryption Profile	Attach a decryption profile to the policy rule in order to block and control certain aspects of the traffic. For details on creating a decryption profile, select Objects > Decryption Profile.
Log Settings	
Log Successful SSL Handshake	(Optional) Creates detailed logs of successful SSL Decryption handshakes. Disabled by default. *Logs consume storage space. Before you log successful SSL handshakes, ensure you have the resources available to store the logs. Edit Device > Setup > Management > Logging and Reporting*

Field	Description
	Settings to check the current log memory allocation to and re-allocate log memory among log types.
Log Unsuccessful SSL Handshake	Creates detailed logs of unsuccessful SSL Decryption handshakes so you can find the cause of decryption issues. Enabled by default.  *Logs consume storage space. To allocate more (or less) log storage space to Decryption logs, edit the log memory allocation (Device > Setup > Management > Logging and Reporting Settings).*
Log Forwarding	Specify the method and location to forward GlobalProtect SSL handshake (decryption) logs.

Decryption Target Tab

- (Panorama only) **Policies** > **Decryption** > **Target**

Select the **Target** tab to select which managed firewalls in the device group to push the policy rule to. You can specify which managed firewalls to push to by select the managed firewalls or by specifying a tag. Additionally, you can configure the policy rule target to push to all managed firewalls except for those specified.

NAT Rule - Target Settings	Description
Any (target all devices)	Enable (check) to push the policy rule to all managed firewalls in the device group.
Devices	Select one or more managed firewalls associated with the device group to push the policy rule to.
Tags	**Add** one or more tags to push the policy rule to managed firewalls in the device group with the specified tag.
Target to all but these specified devices and tags	Enable (check) to push the policy rule to all managed firewalls associated with the device group except for the selected device(s) and tag(s).

Policies > Tunnel Inspection

You can configure the firewall to inspect the traffic content of the following cleartext tunnel protocols:

- Generic Routing Encapsulation (GRE)
- General Packet Radio Service (GPRS) Tunneling Protocol for User Data (GTP-U); supported only on firewalls that support GTP.
- Non-encrypted IPSec traffic (NULL Encryption Algorithm for IPSec and transport mode AH IPSec)
- Virtual Extensible LAN (VXLAN)

You can use tunnel content inspection to enforce Security, DoS Protection, and QoS policies on traffic in these types of tunnels and on traffic nested within another cleartext tunnel (for example, Null Encrypted IPSec inside a GRE tunnel).

Create a Tunnel Inspection policy that, when matching an incoming packet, determines which tunnel protocols in the packet the firewall will inspect and that specifies the conditions under which the firewall drops or continues to process the packet. You can view tunnel inspection logs and tunnel activity in the ACC to verify that tunneled traffic complies with your corporate security and usage policies.

The firewall supports tunnel content inspection on Ethernet interfaces and subinterfaces, AE interfaces, VLAN interfaces, and VPN and LSVPN tunnels. The feature is supported in Layer 3, Layer 2, virtual wire, and tap deployments. Tunnel content inspection works on shared gateways and on virtual system-to-virtual system communications.

What do you want to know?	See:
What are the fields available to create a Tunnel Inspection policy?	Building Blocks in a Tunnel Inspection Policy
How can I view tunnel inspection logs?	Log Types and Severity Levels
Looking for more?	Tunnel Content Inspection

Building Blocks in a Tunnel Inspection Policy

Select **Policies** > **Tunnel Inspection** to add a Tunnel Inspection policy rule. You can use the firewall to inspect content of cleartext tunnel protocols (GRE, GTP-U, non-encrypted IPSec, and VXLAN) and leverage tunnel content inspection to enforce Security, DoS Protection, and QoS policies on traffic in these types of tunnels. All firewall models support tunnel content inspection of GRE and non-encrypted IPSec tunnels, but only firewalls that support GTP support tunnel content inspection of GTP-U tunnels. The following table describes the fields you configure for a Tunnel Inspection policy.

Building Blocks in a Tunnel Inspection Policy	Configured In	Description
Name	**General**	Enter a name for the Tunnel Inspection policy beginning with an alphanumeric character and containing zero or more alphanumeric, underscore, hyphen, period, or space characters.

Building Blocks in a Tunnel Inspection Policy	Configured In	Description
Description		(Optional) Enter a description for the Tunnel Inspection policy.
Tags		(Optional) Enter one or more tags for reporting and logging purposes that identify the packets that are subject to the Tunnel Inspection policy.
Group Rules by Tag		Enter a tag with which to group similar policy rules. The group tag allows you to view your policy rule base based on these tags. You can group rules based on a **Tag**.
Audit Comment		Enter a comment to audit the creation or editing of the policy rule. The audit comment is case-sensitive and can have up to 256 characters, which can be letters, numbers, spaces, hyphens, and underscores.
Audit Comment Archive		View previous **Audit Comments** for the policy rule. You can export the Audit Comment Archive in CSV format.
Source Zone	**Source**	**Add** one or more source zones of packets to which the Tunnel Inspection policy applies (default is **Any**).
Source Address		(Optional) **Add** source IPv4 or IPv6 addresses, address groups, or Geo Region address objects of packets to which the Tunnel Inspection policy applies (default is **Any**).
Source User		(Optional) **Add** source users of packets to which the Tunnel Inspection policy applies (default is **any**).
Negate		(Optional) Select **Negate** to choose any addresses except those specified.
Destination Zone	**Destination**	**Add** one or more destination zones of packets to which the Tunnel Inspection policy applies (default is **Any**).
Destination Address		(Optional) **Add** destination IPv4 or IPv6 addresses, address groups, or Geo Region address objects of packets to which the Tunnel Inspection policy applies (default is **Any**).
Negate		(Optional) Select **Negate** to choose any addresses except those specified.
Tunnel Protocol	**Inspection**	**Add** one or more tunnel **Protocols** that you want the firewall to inspect: • **GRE**—Firewall inspects packets that use Generic Route Encapsulation in the tunnel.

Building Blocks in a Tunnel Inspection Policy	Configured In	Description
		• **GTP-U**—Firewall inspects packets that use the General Packet Radio Service (GPRS) tunneling protocol for user data (GTP-U) in the tunnel. • **Non-encrypted IPSec**—Firewall inspects packets that use non-encrypted IPSec (Null Encrypted IPSec or transport mode AH IPSec) in the tunnel. • **VXLAN**—Firewall inspects a VXLAN payload to find the encapsulated content or applications within the tunnel. To remove a protocol from your list, select the protocol and **Delete** it.
Maximum Tunnel Inspection Levels	**Inspection** > **Inspect Options**	Specify whether the firewall will inspect **One Level** (default) or **Two Levels (Tunnel In Tunnel)** of encapsulation. For VXLAN, select **One Level**, as inspection only occurs on the outer layer.
Drop packet if over maximum tunnel inspection level		(Optional) Drop packets that contain more levels of encapsulation than you specified for Maximum Tunnel Inspection Levels.
Drop packet if tunnel protocol fails strict header check		(Optional) Drop packets that contain a tunnel protocol that uses a header that is non-compliant with the RFC for that protocol. Non-compliant headers indicate suspicious packets. This option causes the firewall to verify GRE headers against RFC 2890. *Do not enable this option if your firewall is tunneling GRE with a device that implements a version of GRE older than RFC 2890.*
Drop packet if unknown protocol inside tunnel		(Optional) Drop packets that contain a protocol inside the tunnel that the firewall cannot identify.
Return Scanned VXLAN Tunnel to Source		(Optional) Enable this option to return the traffic to the originating VXLAN tunnel endpoint (VTEP). For example, use this option to return the encapsulated packet to the source VTEP. Supported only on Layer 3, Layer 3 subinterface, aggregate-interface Layer 3, and VLAN.
Enable Security Options	**Inspection** > **Security Options**	(Optional) **Enable Security Options** to assign security zones for separate Security policy treatment of tunnel content. The inner content source will belong to the **Tunnel Source Zone** you specify and the inner content destination will belong to the **Tunnel Destination Zone** you specify.

Building Blocks in a Tunnel Inspection Policy	Configured In	Description
		If you do not **Enable Security Options**, by default the inner content source belongs to the same zone as the outer tunnel source, and the inner content destination belongs to the same zone as the outer tunnel destination. Therefore, both the inner content source and destination are subject to the same Security policies that apply to the source and destination zones of the outer tunnel.
Tunnel Source Zone		If you **Enable Security Options**, select a tunnel zone that you created, and the inner content will use this source zone for the purpose of policy enforcement. Otherwise, by default the inner content source belongs to the same zone as the outer tunnel source, and the policies of the outer tunnel source zone apply to the inner content source zone also.
Tunnel Destination Zone		If you **Enable Security Options**, select a tunnel zone that you created, and the inner content will use this destination zone for the purpose of policy enforcement. Otherwise, by default the inner content destination belongs to the same zone as the outer tunnel destination, and the policies of the outer tunnel destination zone apply to the inner content destination zone also.
Monitor Name	**Inspection** > **Monitor Options**	(Optional) Enter a monitor name to group similar traffic together for monitoring the traffic in logs and reports.
Monitor Tag (number)		(Optional) Enter a monitor tag number that can group similar traffic together for logging and reporting (range is 1 to 16,777,215). The tag number is globally defined. *This field does not apply to the VXLAN protocol. VXLAN logs automatically use the VXLAN Network Identifier (VNI) from the VXLAN header.*
Log at Session Start		(Optional) Select this option to generate a log at the start of a cleartext tunnel session that matches the Tunnel Inspection policy. This setting overrides the Log at Session Start setting in the Security Policy rule that applies to the session. Tunnel logs are stored separately from traffic logs. The information with the outer tunnel session (GRE, non-encrypted IPSec, or GTP-U) is stored in the Tunnel logs and the inner traffic flows are stored in the Traffic logs. This separation allows you to easily report on tunnel activity (as opposed to inner content activity) with the ACC and reporting features.

Building Blocks in a Tunnel Inspection Policy	Configured In	Description
		The best practice for Tunnel logs is to Log at Session Start and Log at Session End because, for logging, tunnels can be very long-lived. For example, GRE tunnels can come up when the router boots and never terminate until the router is rebooted. If you don't select Log at Session Start, you will never see that there is an active GRE tunnel in the ACC.
Log at Session End		(Optional) Select this option to capture a log at the end of a cleartext tunnel session that matches the Tunnel Inspection policy. This setting overrides the Log at Session End setting in the Security Policy rule that applies to the session.
Log Forwarding		(Optional) Select a Log Forwarding profile from the drop-down to specify where to forward tunnel inspection logs. (This setting is separate from the Log Forwarding setting in a Security policy rule, which applies to traffic logs.)
Name	**Tunnel ID** By default, if you do **not** configure a VXLAN ID, all traffic is inspected. If you configure a VXLAN ID you can use it as a matching criteria to restrict traffic inspection to specific VNIs.	(Optional) A name beginning with an alphanumeric character and containing zero or more alphanumeric, underscore, hyphen, period, and space characters. The **Name** describes the VNIs you are grouping. The name is a convenience, and is not a factor in logging, monitoring, or reporting.
VXLAN ID (VNI)		(Optional) Enter a single VNI, a comma-separated list of VNIs, a range of up to 16 million VNIs (with a hyphen as the separator), or a combination of these. For example: 1-54,1024,1677011-1677038,94 The maximum VXLAN IDs per policy is 4,096. To preserve configuration memory, use ranges where possible.
Any (target all devices) Panorama only	**Target**	Enable (check) to push the policy rule to all managed firewalls in the device group.
Devices Panorama only		Select one or more managed firewalls associated with the device group to push the policy rule to.
Tags Panorama only		**Add** one or more tags to push the policy rule to managed firewalls in the device group with the specified tag.

Building Blocks in a Tunnel Inspection Policy	Configured In	Description
Target to all but these specified devices and tags Panorama only		Enable (check) to push the policy rule to all managed firewalls associated with the device group except for the selected device(s) and tag(s).

Policies > Application Override

To change how the firewall classifies network traffic into applications, you can specify application override policies. For example, if you want to control one of your custom applications, an application override policy can be used to identify traffic for that application according to zone, source and destination address, port, and protocol. If you have network applications that are classified as "unknown," you can create new application definitions for them (refer to Defining Applications).

If possible, avoid using application override policies because they prevent the firewall from using App-ID to identify applications and from performing layer 7 inspection for threats. To support internal proprietary applications, it's better to create custom applications *that include the application signature so the firewall performs layer 7 inspection and scans the application traffic for threats. If a commercial application doesn't have an App-ID,* submit a request for a new App-ID. *If a public application definition (default ports or signature) changes so the firewall no longer identifies the application correctly, create a support ticket so Palo Alto Networks can update the definition. In the meantime, create a custom application so the firewall continues to perform layer 7 inspection of the traffic.*

Like security policies, application override policies can be as general or specific as needed. The policy rules are compared against the traffic in sequence, so the more specific rules must precede the more general ones.

Because the App-ID engine in PAN-OS classifies traffic by identifying the application-specific content in network traffic, the custom application definition cannot simply use a port number to identify an application. The application definition must also include traffic (restricted by source zone, source IP address, destination zone, and destination IP address).

To create a custom application with application override:

- Create a custom application (see Defining Applications). It is not required to specify signatures for the application if the application is used only for application override rules.
- Define an application override policy that specifies when the custom application should be invoked. A policy typically includes the IP address of the server running the custom application and a restricted set of source IP addresses or a source zone.

Use the following tables to configure an application override rule.

- Application Override General Tab
- Application Override Source Tab
- Application Override Destination Tab
- Application Override Protocol/Application Tab
- (Panorama only) Application Override Target Tab

Looking for more?

See Use Application Objects in Policy

Application Override General Tab

Select the **General** tab to configure a name and description for the application override policy. A tag can also be configured to allow you to sort or filter policies when a large number of policies exist.

Field	Description
Name	Enter a name to identify the rule. The name is case-sensitive and can have up to 63 characters, which can be letters, numbers, spaces, hyphens, and underscores. The name must be unique on a firewall and, on Panorama, unique within its device group and any ancestor or descendant device groups.
Description	Enter a description for the rule (up to 1024 characters).
Tag	If you need to tag the policy, **Add** and specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.
Group Rules by Tag	Enter a tag with which to group similar policy rules. The group tag allows you to view your policy rule base based on these tags. You can select to group rules based on a **Tag**.
Audit Comment	Enter a comment to audit the creation or editing of the policy rule. The audit comment s case-sensitive and can have up to 256 characters, which can be letters, numbers, spaces, hyphens, and underscores.
Audit Comment Archive	View previous **Audit Comments** for the policy rule. Audit Comment Archive can be exported in CSV format.

Application Override Source Tab

Select the **Source** tab to define the source zone or source address that defines the incoming source traffic to which the application override policy will be applied.

Field	Description
Source Zone	**Add** source zones (default is **any**). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.
Source Address	**Add** source addresses, address groups, or regions (default is **any**). Select from the drop-down, or click **Address**, **Address Group**, or **Regions** at the bottom of the drop-down, and specify the settings. Select **Negate** to choose any address except the configured ones.

Application Override Destination Tab

Select the **Destination** tab to define the destination zone or destination address that defines the destination traffic to which the policy will be applied.

Field	Description
Destination Zone	Click **Add** to choose destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.
Destination Address	Click **Add** to add destination addresses, address groups, or regions (default is any). Select from the drop-down, or click **Address**, **Address Group**, or **Regions** at the bottom of the drop-down, and specify the settings. Select **Negate** to choose any address except the configured ones.

Application Override Protocol/Application Tab

Select the **Protocol/Application** tab to define the protocol (TCP or UDP), port, and application that further defines the attributes of the application for the policy match.

Field	Description
Protocol	Select the protocol (**TCP** or **UDP**) for which to allow an application override.
Port	Enter the port number (0 to 65535) or range of port numbers (port1-port2) for the specified destination addresses. Multiple ports or ranges must be separated by commas.
Application	Select the override application for traffic flows that match the above rule criteria. When overriding to a custom application, there is no threat inspection that is performed. The exception to this is when you override to a pre-defined application that supports threat inspection. To define new applications, refer to Objects > Applications).

Application Override Target Tab

- (Panorama only) **Policies** > **Application Override** > **Target**

Select the **Target** tab to select which managed firewalls in the device group to push the policy rule to. You can specify which managed firewalls to push to by select the managed firewalls or by specifying a tag. Additionally, you can configure the policy rule target to push to all managed firewalls except for those specified.

NAT Rule - Target Settings	Description
Any (target all devices)	Enable (check) to push the policy rule to all managed firewalls in the device group.
Devices	Select one or more managed firewalls associated with the device group to push the policy rule to.
Tags	**Add** one or more tags to push the policy rule to managed firewalls in the device group with the specified tag.
Target to all but these specified devices and tags	Enable (check) to push the policy rule to all managed firewalls associated with the device group except for the selected device(s) and tag(s).

Policies > Authentication

Your Authentication policy enables you to authenticate end users before they can access network resources.

What do you want to know?	See:
What are the fields available to create an Authentication rule?	Building Blocks of an Authentication Policy Rule
How can I use the web interface to manage Authentication policy?	Create and Manage Authentication Policy For Panorama, see Move or Clone a Policy Rule
Looking for more?	Authentication Policy

Building Blocks of an Authentication Policy Rule

Whenever a user requests a resource (such as when visiting a web page), the firewall evaluates Authentication policy. Based on the matching policy rule, the firewall then prompts the user to respond to one or more challenges of different factors (types), such as login and password, voice, SMS, push, or one-time password (OTP) authentication. After the user responds to all the factors, the firewall evaluates Security policy (see Policies > Security) to determine whether to allow access to the resource.

The firewall does not prompt users to authenticate if they access non-web-based resources (such as a printer) through a GlobalProtect™ gateway that is internal or in tunnel mode. Instead, the users will see connection failure messages. To ensure users can access these resources, set up an authentication portal and train users to visit it when they see connection failures. Consult your IT department to set up an authentication portal.

The following table describes each building block or component in an Authentication policy rule. Before you Add a rule, complete the prerequisites described in Create and Manage Authentication Policy.

Building Blocks in an Authentication Rule	Configured In	Description
Rule number	N/A	Each rule is automatically numbered and the order changes as rules are moved. When you filter rules to match specific filters, the **Policies** > **Authentication** page lists each rule with its number in the context of the complete set of rules in the rulebase and its place in the evaluation order. For details, see rule sequence and its evaluation order.
Name	**General**	Enter a name to identify the rule. The name is case-sensitive and can have up to 63 characters, which can be letters, numbers, spaces, hyphens, and underscores. The name must be unique on a firewall and, on

Building Blocks in an Authentication Rule	Configured In	Description
		Panorama, unique within its device group and any ancestor or descendant device groups.
Description		Enter a description for the rule (up to 1024 characters).
Tag		Select a tag for sorting and filtering rules (see Objects > Tags).
Group Rules by Tag		Enter a tag with which to group similar policy rules. The group tag allows you to view your policy rule base based on these tags. You can group rules based on a **Tag**.
Audit Comment		Enter a comment to audit the creation or editing of the policy rule. The audit comment is case-sensitive and can have up to 256 characters, which can be letters, numbers, spaces, hyphens, and underscores.
Audit Comment Archive		View previous **Audit Comments** for the policy rule. You can export the Audit Comment Archive in CSV format.
Source Zone	**Source**	**Add** zones to apply the rule only to traffic coming from interfaces in the zones that you specify (default is **any**). To define new zones, see Network > Zones.
Source Address		**Add** addresses or address groups to apply the rule only to traffic originating from the sources that you specify (default is **any**). Select **Negate** to choose any address except the selected ones. To define new address or address groups, see Objects > Addresses and Objects > Address Groups.
Source User	**User**	Select the source users or user groups to which the rule applies: • **any**—Includes any traffic regardless of source user. • **pre-logon**—Includes remote users who are not logged into their client systems but whose client systems connect to the network through the GlobalProtect pre-logon feature. • **known-user**—Includes all users for whom the firewall already has IP address-to-username mappings before the rule evokes authentication. • **unknown**—Includes all users for whom the firewall does not have IP address-to-username mappings. After the rule evokes authentication, the firewall

Building Blocks in an Authentication Rule	Configured In	Description
		creates user mappings for unknown users based on the usernames they entered. • **Select**—Includes only the users and user groups that you **Add** to the Source User list.  *If the firewall collects user information from a RADIUS, TACACS+, or SAML identity provider server and not from the User-ID™ agent, the list of users does not display; you must enter user information manually.*
Source HIP Profile		**Add** host information profiles (HIP) to enable you to collect information about the security status of your end hosts, such as whether they have the latest security patches and antivirus definitions. For details and to define new HIPs, see Objects > GlobalProtect > HIP Profiles.
Destination Zone	**Destination**	**Add** zones to apply the rule only to traffic going to interfaces in the zones that you specify (default is **any**). To define new zones, see Network > Zones.
Destination Address		**Add** addresses or address groups to apply the rule only to the destinations that you specify (default is **any**). Select **Negate** to choose any address except the selected ones. To define new address or address groups, see Objects > Addresses and Objects > Address Groups.
Service	**Service/URL Category**	Select from the following options to apply the rule only to services on specific TCP and UDP port numbers: • **any**—Specifies services on any port and using any protocol. • **default**—Specifies services only on the default ports that Palo Alto Networks defines. • **Select**—Enables you to **Add** services or service groups. To create new services and service groups, see Objects > Services and Objects > Service Groups.  *The default selection is service-http. When you use the Authentication policy for Authentication Portal, also enable service-https to ensure that the firewall learns user-to-ip-address mapping for all web traffic.*

Building Blocks in an Authentication Rule	Configured In	Description
URL Category		Select the URL categories to which the rule applies: • Select **any** to specify all traffic regardless of the URL category. • **Add** categories. To define custom categories, see Objects > Custom Objects > URL Category.
Authentication Enforcement	**Actions**	Select the authentication enforcement object (Objects > Authentication) that specifies the method (such as Authentication Portal or browser challenge) and authentication profile that the firewall uses to authenticate users. The authentication profile defines whether users respond to a single challenge or to multi-factor authentication (see Device > Authentication Profile). You can select a predefined or custom authentication enforcement object.  *If you must exclude hosts or servers from a Authentication Portal policy, add them to an Authentication Profile that specifies no-captive-portal as the Authentication Enforcement. However, Authentication Portal policies help the firewall learn user-to-IP-address mapping and should be used when possible.*
Timeout		To reduce the frequency of authentication challenges that interrupt the user workflow, you can specify the interval in minutes (default is 60) when the firewall prompts the user to authenticate only once for repeated access to resources. If the **Authentication Enforcement** object specifies multi-factor authentication, the user must authenticate once for each factor. The firewall records a timestamp and reissues a challenge only when the timeout for a factor expires. Redistributing the timestamps to other firewalls enables you to apply the timeout even if the firewall that initially allows access for a user is not the same firewall that later controls access for that user.  *Timeout is a tradeoff between tighter security (less time between authentication prompts) and the user experience (more time between authentication prompts). More frequent authentication is often the right choice for access to critical systems and*

Building Blocks in an Authentication Rule	Configured In	Description
		sensitive areas such as a data center. Less frequent authentication is often the right choice at the network perimeter and for businesses for which the user experience is key. *For perimeter resources, set the value to 480 minutes (8 hours) and for data center resources and critical systems, set a lower value such as 60 minutes to tighten security. Monitor and adjust the values as necessary.*
Log Authentication Timeouts		Select this option (disabled by default) if you want the firewall to generate Authentication logs whenever the **Timeout** associated with an authentication factor expires. Enabling this option provides more data to troubleshoot access issues. In conjunction with correlation objects, you can also use Authentication logs to identify suspicious activity on your network (such as brute force attacks). *Enabling this option increases log traffic.*
Log Forwarding		Select a Log Forwarding profile if you want the firewall to forward Authentication logs to Panorama or to external services such as a syslog server (see Objects > Log Forwarding).
Any (target all devices) Panorama only	**Target**	Enable (check) to push the policy rule to all managed firewalls in the device group.
Devices Panorama only		Select one or more managed firewalls associated with the device group to push the policy rule to.
Tags Panorama only		**Add** one or more tags to push the policy rule to managed firewalls in the device group with the specified tag.
Target to all but these specified devices and tags Panorama only		Enable (check) to push the policy rule to all managed firewalls associated with the device group except for the selected device(s) and tag(s).

Create and Manage Authentication Policy

Select the **Policies** > **Authentication** page to create and manage Authentication policy rules:

Task	Description
Add	Perform the following prerequisites before creating Authentication policy rules: ❑ Configure the User-ID™ Authentication Portal settings (see Device > User Identification > Authentication Portal Settings). The firewall uses Authentication Portal to display the first authentication factor that the Authentication rule requires. Authentication Portal also enables the firewall to record the timestamps associated with authentication Timeout periods and to update user mappings. ❑ Configure a server profile that specifies how the firewall can access the service that will authenticate users (see Device > Server Profiles). ❑ Assign the server profile to an authentication profile that specifies authentication settings (see Device > Authentication Profile). ❑ Assign the authentication profile to an authentication enforcement object that specifies the authentication method (see Objects > Authentication). To create a rule, perform one of the following steps and then complete the fields described in Building Blocks of an Authentication Policy Rule: • Click **Add**. • Select a rule on which to base the new rule and click **Clone Rule**. The firewall inserts the copied rule, named <rulename>#, below the selected rule, where # is the next available integer that makes the rule name unique, and generates a new UUID for the cloned rule. For details, see Move or Clone a Policy Rule.
Modify	To modify a rule, click the rule Name and edit the fields described in Building Blocks of an Authentication Policy Rule. *If the firewall received the rule from Panorama, the rule is read-only; you can edit it only on Panorama.*
Move	When matching traffic, the firewall evaluates rules from top to bottom in the order that the **Policies** > **Authentication** page lists them. To change the evaluation order, select a rule and **Move Up**, **Move Down**, **Move Top**, or **Move Bottom**. For details, see Move or Clone a Policy Rule.
Delete	To remove an existing rule, select and **Delete** it.
Enable/Disable	To disable a rule, select and **Disable** it. To re-enable a disabled rule, select and **Enable** it.
Highlight Unused Rules	To identify rules that have not matched traffic since the last time the firewall was restarted, **Highlight Unused Rules**. You can then decide whether to disable or delete unused rules. The page highlights unused rules with a dotted yellow background.
Preview rules (Panorama only)	Click **Preview Rules** to view a list of the rules before you push the rules to the managed firewalls. Within each rulebase, the page visually demarcates the rule hierarchy for each device group (and managed firewall) to facilitate scanning of numerous rules.

Policies > DoS Protection

A DoS Protection policy allows you to protect individual critical resources against DoS attacks by specifying whether to deny or allow packets that match a source interface, zone, address or user and/or a destination interface, zone, or user.

Alternatively, you can choose the Protect action and specify a DoS profile where you set the thresholds (sessions or packets per second) that trigger an alarm, activate a protective action, and indicate the maximum rate above which all new connections are dropped. Thus, you can control the number of sessions between interfaces, zones, addresses, and countries based on aggregate sessions or source and/or destination IP addresses. For example, you can control traffic to and from certain addresses or address groups, or from certain users and for certain services.

The firewall enforces DoS Protection policy rules before Security policy rules to ensure the firewall uses its resources in the most efficient manner. If a DoS Protection policy rule denies a packet, that packet never reaches a Security policy rule.

The following tables describe the DoS Protection policy settings:

- DoS Protection General Tab
- DoS Protection Source Tab
- DoS Protection Destination Tab
- DoS Protection Option/Protection Tab
- (Panorama only) DoS Protection Target Tab

Looking for more?

See DoS Protection Profiles and Objects > Security Profiles > DoS Protection.

DoS Protection General Tab

- **Policies** > **DoS Protection** > **General**

Select the **General** tab to configure a name and description for the DoS Protection policy. You can also configure a tag to allow you to sort or filter policies when many policies exist.

Field	Description
Name	Enter a name to identify the DoS Protection policy rule. The name is case-sensitive and can have up to 63 characters, which can be letters, numbers, spaces, hyphens, and underscores. The name must be unique on a firewall and, on Panorama, unique within its device group and any ancestor or descendant device groups.
Description	Enter a description for the rule (up to 1024 characters).
Tags	If you want to tag the policy, **Add** and specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. A tag is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt or No-decrypt, or use the name of a specific data center for policies associated with that location.
Group Rules by Tag	Enter a tag with which to group similar policy rules. The group tag allows you to view your policy rule base based on these tags. You can group rules based on a **Tag**.

Field	Description
Audit Comment	Enter a comment to audit the creation or editing of the policy rule. The audit comment is case-sensitive and can have up to 256 characters, which can be letters, numbers, spaces, hyphens, and underscores.
Audit Comment Archive	View previous **Audit Comments** for the policy rule. You can export the Audit Comment Archive in CSV format.

DoS Protection Source Tab

Select the **Source** tab to define the source interface(s) or source zone(s), and optionally the source address(es) and source user(s) that define the incoming traffic to which the DoS policy rule applies.

Field	Description
Type	Select the type of source to which the DoS Protection policy rule applies: • **Interface** —Apply the rule to traffic coming from the specified interface or group of interfaces. • **Zone**—Apply the rule to traffic coming from any interface in a specified zone. Click **Add** to select multiple interfaces or zones.
Source Address	Select **Any** or **Add** and specify one or more source addresses to which the DoS Protection policy rule applies. (Optional) Select **Negate** to specify that the rule applies to any addresses except those specified.
Source User	Specify one or more source users to which the DoS Protection policy rule applies: • **any**—Includes packets regardless of the source user. • **pre-logon**—Includes packets from remote users that are connected to the network using GlobalProtect, but are not logged into their system. When **pre-logon** is configured on the Portal for GlobalProtect apps, any user who is not currently logged into their machine will be identified with the username pre-logon. You can then create policies for pre-logon users and although the user is not directly logged in, their machines are authenticated on the domain as if they were fully logged in. • **known-user**—Includes all authenticated users, which means any IP address with user data mapped. This option is equivalent to the “domain users” group on a domain. • **unknown**—Includes all unauthenticated users, which means IP addresses that are not mapped to a user. For example, you could use **unknown** for guest level access to something because they will have an IP address on your network, but will not be authenticated to the domain and will not have IP address-to-username mapping information on the firewall. • **Select**—Includes users specified in this window. For example, you can select one user, a list of individuals, some groups, or manually add users. *If the firewall collects user information from a RADIUS, TACACS+, or SAML identity provider server and not from the User-ID™ agent,*

Field	Description
	the list of users does not display; you must enter user information manually.

DoS Protection Destination Tab

Select the **Destination** tab to define the destination zone or interface and destination address that define the destination traffic to which the policy applies.

Field	Description
Type	Select the type of destination to which the DoS Protection policy rule applies: • **Interface**—Apply the rule to packets going to the specified interface or group of interfaces. Click **Add** and select one or more interfaces. • **Zone**—Apply the rule to packets going to any interface in the specified zone. Click **Add** and select one or more zones.
Destination Address	Select **Any** or **Add** and specify one or more destination addresses to which the DoS Protection policy rule applies. (Optional) Select **Negate** to specify that the rule applies to any addresses except those specified.

DoS Protection Option/Protection Tab

Select the **Option/Protection** tab to configure options for the DoS Protection policy rule, such as the type of service to which the rule applies, the action to take against packets that match the rule, and whether to trigger log forwarding for matched traffic. You can define a schedule for when the rule is active.

You can also select an aggregate DoS Protection profile and/or a classified DoS Protection profile, which determine the threshold rates that, when exceeded, cause the firewall to take protective actions, such as trigger an alarm, activate an action such as Random Early Drop, and drop packets that exceed the maximum threshold rate.

Field	Description
Service	Click **Add** and select one or more services to which the DoS Protection policy applies. The default is **Any** service. For example, if the DoS policy protects web servers, specify HTTP, HTTPS, and any other appropriate service ports for the web applications.  *For critical servers, create separate DoS Protection rules to protect the unused service ports to help prevent targeted attacks.*
Action	Select the action the firewall performs on packets that match the DoS Protection policy rule: • **Deny**—Drop all packets that match the rule. • **Allow**—Permit all packets that match the rule.

Field	Description
	• **Protect**—Enforce the protections specified in the specified DoS Protection profile on packets that match the rule. Packets that match the rule are counted toward the threshold rates in the DoS Protection profile, which in turn trigger an alarm, activate another action, and trigger packet drops when the maximum rate is exceeded.  *The object of applying DoS Protection is to protect against DoS attacks, so you should use usually Protect. Deny drops legitimate traffic along with DoS traffic and Allow doesn't stop DoS attacks. Use Deny and Allow only to make exceptions within a group. For example, you can deny the traffic from most of a group but allow a subset of that traffic, or allow the traffic from most of a group but deny a subset of that traffic.*
Schedule	Specify the schedule when the DoS Protection policy rule is in effect. The default setting of **None** indicates no schedule; the policy is always in effect. Alternatively, select a schedule or create a new schedule to control when the DoS Protection policy rule is in effect. Enter a **Name** for the schedule. Select **Shared** to share this schedule with every virtual system on a multiple virtual system firewall. Select a **Recurrence** of **Daily**, **Weekly**, or **Non-recurring**. Add a **Start Time** and **End Time** in hours:minutes, based on a 24-hour clock.
Log Forwarding	If you want to trigger forwarding of threat log entries for matched traffic to an external service, such as to a syslog server or Panorama, select a Log Forwarding profile or click **Profile** to create a new one.  *The firewall logs and forwards only traffic that matches an action in the rule.*  *For easier management, forward DoS logs separately from other Threat logs, both directly to administrators via email and to a log server.*
Aggregate	Aggregate DoS Protection profiles set thresholds that apply to combined group of devices specified in the DoS Protection rule to protect those server groups. For example, an Alarm Rate threshold of 10,000 CPS means that when the total new CPS to the entire group exceeds 10,000 CPS, the firewall triggers an alarm message. Select an Aggregate DoS Protection profile that specifies the threshold rates at which the incoming connections per second trigger an alarm, activate an action, and exceed a maximum rate. All incoming connections (the aggregate) count toward the thresholds specified in an Aggregate DoS Protection profile. An Aggregate profile setting of **None** means there are no threshold settings in place for the aggregate traffic. See Objects > Security Profiles > DoS Protection.
Classified	Classified DoS Protection profiles set thresholds that apply to each individual device specified in the DoS Protection rule to protect individual or small groups of critical servers. For example, an Alarm Rate threshold of 10,000 CPS means that when the total new CPS to any individual server specified in the rule exceeds 10,000 CPS, the firewall triggers an alarm message.

Field	Description
	Select this option and specify the following: • **Profile**—Select a Classified DoS Protection profile to apply to this rule. • **Address**—Select whether incoming connections count toward the thresholds in the profile if they match the **source-ip-only**, **destination-ip-only**, or **src-dest-ip-both**.  *The firewall consumes more resources to track src-dest-ip-both counters than to track only the source IP or only the destination IP counters.* If you specify a Classified DoS Protection profile, only the incoming connections that match a source IP address, destination IP address, or source and destination IP address pair count toward the thresholds specified in the profile. For example, you can specify a Classified DoS Protection profile with a **Max Rate** of 100 cps, and specify an **Address** setting of **source-ip-only** in the rule. The result would be a limit of 100 connections per second for that particular source IP address.  *Don't use source-ip-only or src-dest-ip-both for internet-facing zones because the firewall can't store counters for all possible internet IP addresses. Use destination-ip-only in perimeter zones.* *Use destination-ip-only to protect individual critical devices.* *Use source-ip-only and the Alarm threshold to monitor suspect hosts in non-internet-facing zones.* See Objects > Security Profiles > DoS Protection.

DoS Protection Target Tab

- (Panorama only) **Policies** > **DoS Protection** > **Target**

Select the **Target** tab to select which managed firewalls in the device group to push the policy rule to. You can specify which managed firewalls to push to by select the managed firewalls or by specifying a tag. Additionally, you can configure the policy rule target to push to all managed firewalls except for those specified.

NAT Rule - Target Settings	Description
Any (target all devices)	Enable (check) to push the policy rule to all managed firewalls in the device group.
Devices	Select one or more managed firewalls associated with the device group to push the policy rule to.
Tags	**Add** one or more tags to push the policy rule to managed firewalls in the device group with the specified tag.
Target to all but these specified devices and tags	Enable (check) to push the policy rule to all managed firewalls associated with the device group except for the selected device(s) and tag(s).

Policies > SD-WAN

Add a SD-WAN policy to configure the link path management settings on a per-application, or for a group of applications that traverse the same link, based on health jitter, latency, and packet loss health metrics you configure. When certain paths between the source and destination for critical applications experience degradation, the SD-WAN policy rule selects a new optimal path to ensure that the sensitive and critical applications perform according to the path quality profile assigned to it in the SD-WAN policy rule.

- SD-WAN General Tab
- SD-WAN Source Tab
- SD-WAN Destination Tab
- SD-WAN Application/Service Tab
- SD-WAN Path Selection Tab
- (Panorama Only) SD-WAN Target Tab

SD-WAN General Tab

- **Policies** > **SD-WAN** > **General**

Select the **General** tab to configure a name and description for the SD-WAN policy. A tag can also be configured to allow you to sort or filter policies when a large number of policies exist.

Field	Description
Name	Enter a name to identify the rule. The name is case-sensitive and can have up to 63 characters, which can be letters, numbers, spaces, hyphens, and underscores. The name must be unique on a firewall and, on Panorama, unique within its device group and any ancestor or descendant device groups.
Description	Enter a description for the rule (up to 1,024 characters).
Tag	If you need to tag the policy, **Add** and specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain SD-WAN policies with unique tags that identify specific hubs or branches that the rules applies to.
Group Rules by Tag	Enter a tag with which to group similar policy rules. The group tag allows you to view your policy rule base based on these tags. You can select to group rules based on a **Tag**.
Audit Comment	Enter a comment to audit the creation or editing of the policy rule. The audit comment is case-sensitive and can have up to 256 characters, which can be letters, numbers, spaces, hyphens, and underscores.
Audit Comment Archive	View previous **Audit Comments** for the policy rule. Audit Comment Archive can be exported in CSV format.

SD-WAN Source Tab

- **Policies** > **SD-WAN** > **Source**

Select the **Source** tab to define the source zones, source addresses, and source users that define the incoming packets to which the SD-WAN policy applies.

Field	Description
Source Zone	To specify a source zone, select **Add** and select one or more zones, or select **Any** zone. Specifying multiple zones can simplify management. For example, if you have three branches in different zones and you want the remaining match criteria and path selection to be the same for the three branches, you can create one SD-WAN rule and specify the three source zones to cover the three branches. *Only Layer 3 type zones are supported for SD-WAN policy rules.*
Source Address	To specify source addresses, **Add** source addresses or external dynamic lists (EDL), select from the drop-down, or select **Address** and create a new address object. Alternatively, select **Any** source address (default).
Source User	To specify certain users, select **Add** (the type then indicates **select**) and enter a user, list of users, or groups of users. Alternatively, select a type of user: • **any**—(default) Include any user, regardless of user data. • **pre-logon**—Include remote users who are connected to the network using GlobalProtect™, but are not logged into their system. When the Pre-logon option is configured on the Portal for GlobalProtect apps, any user who is not currently logged into their machine will be identified with the username pre-logon. You can then create policies for pre-logon users and although the user is not logged in directly, their machines are authenticated on the domain as if they were fully logged in. • **known-user**—Includes all authenticated users, which means any IP address with user data mapped. This option is equivalent to the "domain users" group on a domain. • **unknown**—Includes all unauthenticated users, which means IP addresses that are not mapped to a user. For example, you could select **unknown** for guest-level access to something because they will have an IP address on your network, but will not be authenticated to the domain and will not have IP address-to-user mapping information on the firewall. *If the firewall collects user information from a RADIUS, TACACS+, or SAML identity provider server and not from the User-ID™ agent, the list of users does not display; you must enter user information manually.*

SD-WAN Destination Tab

- **Policies** > **SD-WAN** > **Destination**

Select the **Destination** tab to define the destination zone(s) or destination address(es) that define the traffic to which the SD-WAN policy rule applies.

Field	Description
Destination Zone	**Add** destination zones (default is any). Zones must be Layer 3. To define new zones, refer to Network > Zones. Add Multiple zones to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.
Destination Address	**Add** destination addresses, address groups, External Dynamic Lists (EDL), or regions (default is **Any**). Select from the drop-down, or click **Address** or **Address Group** at the bottom of the drop-down, and specify the settings. Select **Negate** to choose any address except the configured ones.

SD-WAN Application/Service Tab

- **Policies** > **SD-WAN** > **Application/Service**

Select the **Application/Service** tab to specify the applications or services to which the SD-WAN policy rule applies and to specify profiles (Path Quality, SaaS Quality, and Error Correction profiles) that apply to the applications or services.

Field	Description
Path Quality Profile	Select a path quality profile that determines the maximum jitter, latency and packet loss percentage thresholds you want to apply to the specified applications and services. If a path quality profile has not yet been created, you can create a **New SD-WAN Path Quality Profile**.
SaaS Quality Profile	Select a SaaS quality profile to specify the path quality thresholds for latency, jitter, and packet loss for a hub or branch firewall that has Direct Internet Access (DIA) link to a Software-as-a-Service (SaaS) application. If a SaaS quality profile has not yet been created, you can create a **New SaaS Quality Profile**. Default is **None (disabled)**.
Error Correction Profile	Select an **Error Correction Profile** or create a new Error Correction Profile, which specifies the parameters to control forward error correction (FEC) or path duplication for the applications or services specified in the rule. This profile can be used by either hub or branch firewall. Default is **None (disabled)**.
Applications	**Add** specific applications for the SD-WAN policy rule, or select **Any**. If an application has multiple functions, select the overall application or individual functions. If you select the overall application, all functions

Field	Description
	are included and the application definition is automatically updated as future functions are added. If you are using application groups, filters, or containers in the SD-WAN policy rule, view details of these objects by hovering over the object in the Application column, opening the drop-down, and selecting **Value**. This allows you to view application members directly from the policy without having to navigate to the **Object** tab. *Add only business-critical applications that are affected by latency, jitter, or packet loss. Avoid adding application categories or sub-categories as these are too broad and do not allow for per-application control.*
Service	**Add** specific services for the SD-WAN policy rule and select on which ports packets from these services are allowed or denied: • **any**—The selected services are allowed or denied on any protocol or port. • **application-default**—The selected services are allowed or denied only on their default **ports defined by Palo Alto Networks®**. This option is recommended for policies that specify the **allow** action because it prevents services from running on unusual ports and protocols which, if unintentional, can be a sign of undesired service behavior and usage. *When you use this option, only the default port matches the SD-WAN policy and action is enforced. Other services not on the default port may be allowed depending on the Security policy rule, but do not match the SD-WAN policy, and no SD-WAN policy rule action is taken.* *For most services, use application-default to prevent the service from using non-standard ports or exhibiting other evasive behaviors. If the default port for the service changes, the firewall automatically updates the rule to the correct default port. For services that use non-standard ports, such as internal custom services, either modify the service or create a rule that specifies the non-standard ports and apply the rule only to the traffic that requires the service.* • **Select**—**Add** an existing service or choose **Service** or **Service Group** to specify a new entry. (Or select Objects > Services and Objects > Service Groups).

SD-WAN Path Selection Tab

- **Policies** > **SD-WAN** > **Path Selection**

Select the **Path Selection** tab to define paths for applications or services traffic to swap to if the primary path quality exceeds the configured path quality thresholds in the Path Quality Profile.

Field	Description
Traffic Distribution Profile	From the drop-down select a traffic distribution profile, which determines how the firewall selects an alternate path for the application or service traffic when one of the path health metrics for the preferred path exceeds the threshold configured in the path quality profile for the rule.

SD-WAN Target Tab

- **Policies** > **SD-WAN** > **Target**

Select the **Target** tab to select the managed devices to push the SD-WAN policy rules to. This tab is supported only on the Panorama management server.

Field	Description
Any (target all devices)	Enable (check) to push the SD-WAN policy rule to all devices by the Panorama management server.
Devices	Select one or more devices to which to push the SD-WAN policy rule. You can filter devices based on device state, platform, device group, templates, tags, or HA status.
Tags	Specify the tag for the policy. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain rules with specific words like Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location. You can also add tags to the default rules.
Target to all but these specified devices and tags	Enable (check) to target and push the policy rule to all devices except for the selected **Devices** and **Tags**.

Objects

Objects are the elements that enable you to construct, schedule, and search for policy rules, and Security Profiles provide threat protection in policy rules.

This section describes how to configure the Security Profiles and objects that you can use with Policies:

- Move, Clone, Override, or Revert Objects
- Objects>Addresses
- Objects>Address Groups
- Objects>Regions
- Objects>Applications
- Objects>Application Groups
- Objects>Application Filters
- Objects>Services
- Objects>ServiceGroups
- Objects>Tags
- Objects > Devices
- Objects>GlobalProtect> HIP Objects
- Objects>GlobalProtect> HIP Profiles
- Objects>External Dynamic Lists
- Objects>Custom Objects
- Objects>Security Profiles
- Objects > Security Profiles > Mobile Network Protection
- Objects > Security Profiles > SCTP Protection
- Objects>Security Profile Groups
- Objects>Log Forwarding
- Objects>Authentication
- Objects>Decryption Profile
- Objects > SD-WAN Link Management
- Objects>Schedules

Move, Clone, Override, or Revert Objects

See the following topics for options to modify existing objects:

- Move or Clone an Object
- Override or Revert an Object

Move or Clone an Object

When moving or cloning objects, you can assign a **Destination** (a virtual system on a firewall or a device group on Panorama™) for which you have access permissions, including the Shared location.

To move an object, select the object in the **Objects** tab, click **Move**, select **Move to other vsys** (firewall only) or **Move to other device group** (Panorama only), complete the fields in the following table, and then click **OK**.

To clone an object, select the object in the **Objects** tab, click **Clone**, complete the fields in the following table, and then click **OK**.

Move/Clone Settings	Description
Selected Objects	Displays the Name and current Location (virtual system or device group) of the policies or objects you selected for the operation.
Destination	Select the new location for the policy or object: a virtual system, device group, or Shared. The default value is the **Virtual System** or **Device Group** that you selected in the **Policies** or **Objects** tab.
Error out on first detected error in validation	Select this option (selected by default) to make the firewall or Panorama display the first error it finds and stop checking for more errors. For example, an error occurs if the **Destination** doesn't include an object that is referenced in the policy rule you are moving. If you clear this selection, the firewall or Panorama will find all errors before displaying them.

Override or Revert an Object

In Panorama, you can nest device groups in a tree hierarchy of up to four levels. At the bottom level, a device group can have parent, grandparent, and great-grandparent device groups at successively higher levels—collectively called *ancestors*—from which the bottom-level device group inherits policies and objects. At the top level, a device group can have child, grandchild, and great-grandchild device groups—collectively called *descendants*. You can override an object in a descendant so that its values differ from those in an ancestor. This override capability is enabled by default. However, you cannot override shared or default (preconfigured) objects. The web interface displays the icon to indicate an object has inherited values and displays the icon to indicate an inherited object has overridden values.

- **Override an object**—Select the **Objects** tab, select the descendant **Device Group** that will have the overridden version, select the object, click **Override**, and edit the settings. You cannot override **Name** or **Shared** settings for an object.
- **Revert an overridden object to its inherited values**—Select the **Objects** tab, select the **Device Group** that has the overridden version, select the object, click **Revert**, and click **Yes** to confirm the operation.

- **Disable overrides for an object**—Select the **Objects** tab, select the **Device Group** where the object resides, click the object Name to edit it, select **Disable override**, and click **OK**. Overrides for that object are then disabled in all device groups that inherit the object from the selected **Device Group**.
- **Replace all object overrides across Panorama with the values inherited from the Shared location or ancestor device groups**—Select **Panorama** > **Setup** > **Management**, edit the Panorama Settings, select **Ancestor Objects Take Precedence**, and click **OK**. You must then commit to Panorama and to the device groups containing overrides to push the inherited values.

Objects > Addresses

An address object can include either IPv4 or IPv6 addresses (a single IP address, a range of addresses, or a subnet), an FQDN, or a wildcard address (IPv4 address followed by a slash and wildcard mask). An address object allows you to reuse that same address or group of addresses as a source or destination address in policy rules, filters, and other firewall functions without adding each address manually for each instance. You create an address object using the web interface or CLI; changes require a commit operation to make the object a part of the configuration.

First **Add** a new address object and then specify the following values:

Address Object Settings	Description
Name	Enter a name (up to 63 characters) that describes the addresses you will include as part of this object. This name appears in the address list when defining security policy rules. The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this option if you want to share this address object with: • **Every virtual system (vsys) on a multi-vsys firewall**—If you do not select this option, the address object will be available only to the **Virtual System** selected in the **Objects** tab. • **Every device group on Panorama**—If you do not select this option, the address object will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this address object in device groups that inherit this object. By default, this selection is disabled, which means administrators can override the settings for any device group that inherits the object.
Description	Enter a description for the object (up to 1,023 characters).
Type	Specify the type of address object and the entry: • **IP Netmask**—Enter the IPv4 or IPv6 address or IP address range using the following notation: *ip_address/mask* or *ip_address* where the mask is the number of significant binary digits used for the network portion of the address. Ideally, for IPv6 addresses, you specify only the network portion, not the host portion. For example: • **192.168.80.150/32**—Indicates one address. • **192.168.80.0/24**—Indicates all addresses from 192.168.80.0 through 192.168.80.255. • **2001:db8::/32** • **2001:db8:123:1::/64** • **IP Range**—Enter a range of addresses using the following format: *ip_address-ip_address* where both ends of the range are IPv4 addresses or both are IPv6 addresses. For example: 2001:db8:123:1::1-2001:db8:123:1::22 • **IP Wildcard Mask**—Enter an IP wildcard address in the format of an IPv4 address followed by a slash and a mask (which must begin with

Address Object Settings	Description
	a zero); for example, 10.182.1.1/0.127.248.0. In the wildcard mask, a zero (0) bit indicates that the bit being compared must match the bit in the IP address that is covered by the 0. A one (1) bit in the mask is a wildcard bit, meaning the bit being compared need not match the bit in the IP address that is covered by the 1. Convert the IP address and the wildcard mask to binary. To illustrate the matching: on binary snippet 0011, a wildcard mask of 1010 results in four matches (0001, 0011, 1001, and 1011).  *You can use an address object of type IP Wildcard Mask only in a Security policy rule.* • **FQDN**—Enter the domain name. The FQDN initially resolves at commit time. An FQDN entry is subsequently refreshed based on the TTL of the FQDN if the TTL is greater than or equal to the Minimum FQDN Refresh Time; otherwise the FQDN entry is refreshed at the Minimum FQDN Refresh Time. The FQDN is resolved by the system DNS server or a DNS proxy object if a proxy is configured.
Resolve	After selecting the address type and entering an IP address or FQDN, click **Resolve** to see the associated FQDN or IP addresses, respectively (based on the DNS configuration of the firewall or Panorama). You can change an address object from an FQDN to an IP Netmask or vice versa. To change from an FQDN to an IP Netmask, click **Resolve** to see the IP addresses that the FQDN resolves to, then select one and **Use this address**. The address object Type dynamically changes to IP Netmask and the IP address you selected appears in the text field. Alternatively, to change an address object from an IP Netmask to an FQDN, click **Resolve** to see the DNS name that the IP Netmask resolves to, then select the FQDN and **Use this FQDN**. The Type changes to FQDN and the FQDN appears in the text field.
Tags	Select or enter the tags that you want to apply to this address object. You can define a tag here or use the Objects > Tags tab to create new tags.

Objects > Address Groups

To simplify the creation of security policies, addresses that require the same security settings can be combined into address groups. An address group can be static or dynamic.

- Dynamic Address Groups: A dynamic address group populates its members dynamically using looks ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall.

  To use a dynamic address group in policy you must complete the following tasks:

  - Define a dynamic address group and reference it in a policy rule.
  - Notify the firewall of the IP addresses and the corresponding tags, so that members of the dynamic address group can be formed. You can do this using external scripts that use the XML API on the firewall or, for a VMware-based environment, you can select **Device** > **VM Information Sources** to configure settings on the firewall.

  Dynamic address groups can also include statically defined address objects. If you create an address object and apply the same tags that you have assigned to a dynamic address group, that dynamic address group will include all static and dynamic objects that match the tags. You can, therefore use tags to pull together both dynamic and static objects in the same address group.
- Static Address Groups: A static address group can include address objects that are static, dynamic address groups, or it can be a combination of both address objects and dynamic address groups.

  To create an address group, click **Add** and fill in the following fields:

Address Group Settings	Description
Name	Enter a name that describes the address group (up to **63** characters). This name appears in the address list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this option if you want the address group to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the address group will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the address group will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this address group object in device groups that inherit the object. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Description	Enter a description for the object (up to 1023 characters).
Type	Select **Static** or **Dynamic**.

Address Group Settings	Description
	To create a dynamic address group, use the match criteria is assemble the members to be included in the group. Define the **Match** criteria using the **AND** or **OR** operators.  *To view the list of attributes for the match criteria, you must have configured the firewall to access and retrieve the attributes from the source/host. Each virtual machine on the configured information source(s) is registered with the firewall and the firewall can poll the machine to retrieve changes in IP address or configuration without any modifications on the firewall.* For a static address group, click **Add** and select one or more **Addresses**. Click **Add** to add an object or an address group to the address group. The group can contain address objects, and both static and dynamic address groups.
Tags	Select or enter the tags that you wish to apply to this address group. For information on tags, see Objects > Tags.
Members Count and Address	After you add an address group, the Members Count column on the **Objects** > **Address Groups** page indicates whether the objects in the group are populated dynamically or statically. • For a static address group, you can view the count of the members in the address group. • For an address group that uses tags to dynamically populate members or has both static and dynamic members, to view the members, click the **More...** link in the Address column. You can now view the IP addresses that are registered to the address group. • Type indicates whether the IP address is a static address object or being dynamically registered and displays the IP address. • Action allows you to **Unregister Tags** from an IP address. Click the link to **Add** the registration source and specify the tags to unregister.

Objects > Regions

The firewall supports creation of policy rules that apply to specified countries or other regions. The region is available as an option when specifying source and destination for security policies, decryption policies, and DoS policies. You can choose from a standard list of countries or use the region settings described in this section to define custom regions to include as options for Security policy rules.

The following tables describe the region settings:

Region Settings	Description
Name	Select a name that describes the region. This name appears in the address list when defining security policies.
Geo Location	To specify latitude and longitude, select this option and specify the values (xxx.xxxxxx format). This information is used in the traffic and threat maps for App-Scope. Refer to Monitor > Logs.
Addresses	Specify an IP address, range of IP addresses, or subnet to identify the region, using any of the following formats: x.x.x.x x.x.x.x-y.y.y.y x.x.x.x/n

Objects > Dynamic User Groups

To create a dynamic user group, select **Objects** > **Dynamic User Groups**, **Add** a new dynamic user group and then configure the following settings:

Dynamic User Group Settings	Description
Name	Enter a **Name** that describes the dynamic user group (up to 63 characters). This name appears in the source user list when defining Security policy rules. The name must be unique and use only alphanumeric characters, spaces, hyphens, and underscores.
Description	Enter a **Description** for the object (up to 1,023 characters).
Shared (Panorama only)	Select this option if you want the match criteria of the dynamic user group to be available to every device group on Panorama. *Panorama does not share the members of the group with device groups.* If you clear this option, the match criteria of the dynamic user group are available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this dynamic user group in device groups that inherit the object. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Match	**Add Match Criteria** to define the members in the dynamic user group using the **AND** or **OR** operators to include multiple tags. *When you Add Match Criteria, only existing tags display. You can select an existing tag or create new tags.*
Tags	(Optional) Select or enter the static object tags that you want to apply to the dynamic user group object. This tags the dynamic user group object itself, not the members in the group. The tags you select allow you to group related items and are not related to the match criteria. For information on tags, see Objects > Tags.

After you add a dynamic user group, you can view the following information for the group:

Dynamic User Groups Column	Description
Location (Panorama only)	Identifies whether the match criteria for the dynamic user group is available to every device group on Panorama (**Shared**) or to the selected device group.
Users	Select **more** to see the list of users in the dynamic user group.

Dynamic User Groups Column	Description
	• To add tags to users for inclusion in the group, **Register Users**, then select the **Registration Source** and the **Tags** you want to apply to the user. When the user's tags match the criteria for the group, the firewall adds the user to the dynamic user group. • (Optional) Specify a **Timeout** in minutes (default is 0; range is 0 to 43,200) to remove users from the group when the specified time expires. • (Optional) **Add Users** to the group or **Delete** users from the group. • To remove tags from users and prevent them from becoming members of the group, select the users, and **Unregister Users**, and then select **Registration Source** and **Tags**. • When done reviewing or modifying the dynamic user group list of users, click **Close**.

Objects > Applications

The following topics describe the **Applications** page.

What are you looking for?	See
Understand the application settings and attributes displayed on the Applications page.	Applications Overview Actions Supported on Applications
Add a new application or modify an existing application.	Defining Applications

Applications Overview

The Applications page lists various attributes of each application definition, such as the application's relative security risk (1 to 5). The risk value is based on criteria such as whether the application can share files, is prone to misuse, or tries to evade firewalls. Higher values indicate higher risk.

The top application browser area of the page lists the attributes that you can use to filter the display as follows. The number to the left of each entry represents the total number of applications with that attribute.

Weekly content releases periodically include new decoders and contexts for which you can develop signatures.

The following table describes application details—custom applications and Palo Alto® Networks applications might display some or all of these fields.

Application Details	Description
Name	Name of the application.
Description	Description of the application (up to 255 characters).
Additional Information	Links to web sources (Wikipedia, Google, and Yahoo!) that contain additional information about the application.
Standard Ports	Ports that the application uses to communicate with the network.
Depends on	List of other applications that are required for this application to run. When creating a policy rule to allow the selected application, you

Application Details	Description
	must also be sure that you are allowing any other applications that the application depends on.
Implicitly Uses	Other applications that the selected application depends on but that you do not need to add to your Security policy rules to allow the selected application because those applications are supported implicitly.
Previously Identified As	For a new App-ID™, or App-IDs that are changed, this indicates what the application was previously identified as. This helps you assess whether policy changes are required based on changes in the application. If an App-ID is disabled, sessions associated with that application will match policy as the previously identified as application. Similarly, disabled App-IDs will appear in logs as the application they were previous identified as.
Deny Action	App-IDs are developed with a default deny action that dictates how the firewall responds when the application is included in a Security policy rule with a deny action. The default deny action can specify either a silent drop or a TCP reset. You can override this default action in Security policy.
Characteristics	
Evasive	Uses a port or protocol for something other than its originally intended purpose with the hope that it will traverse a firewall.
Excessive Bandwidth	Consumes at least 1 Mbps on a regular basis through normal use.
Prone to Misuse	Often used for nefarious purposes or is easily set up to expose more than the user intended.
SaaS	On the firewall, Software as a Service (SaaS) is characterized as a service where the software and infrastructure are owned and managed by the application service provider but where you retain full control of the data, including who can create, access, share, and transfer the data. Keep in mind that in the context of how an application is characterized, SaaS applications differ from web services. Web services are hosted applications where either the user doesn't own the data (for example, Pandora) or where the service is primarily comprised of sharing data fed by many subscribers for social purposes (for example, LinkedIn, Twitter, or Facebook).
Capable of File Transfer	Has the capability to transfer a file from one system to another over a network.
Tunnels Other Applications	Is able to transport other applications inside its protocol.
Used by Malware	Malware has been known to use the application for propagation, attack, or data theft, or is distributed with malware.

Application Details	Description
Has Known Vulnerabilities	Has publicly reported vulnerabilities.
Pervasive	Likely has more than 1,000,000 users.
Continue Scanning for Other Applications	Instructs the firewall to continue to try and match against other application signatures. If you do not select this option, the firewall stops looking for additional application matches after the first matching signature.
SaaS Characteristics	
Data Breaches	Applications that may have released secure information to an untrusted source within the past three years.
Poor Terms of Service	Applications with unfavorable terms of service that can compromise enterprise data.
No Certifications	Applications lacking current compliance to industry programs or certifications such as SOC1, SOC2, SSAE16, PCI, HIPAA, FINRAA, or FEDRAMP.
Poor Financial Viability	Applications with the potential to be out of business within the next 18 to 24 months.
No IP Restrictions	Applications without IP-based restrictions for user access.
Classification	
Category	The application category will be one of the following: • business-systems • collaboration • general-internet • media • networking • unknown
Subcategory	The subcategory in which the application is classified. Different categories have different subcategories associated with them. For example, subcategories in the collaboration category include email, file-sharing, instant-messaging, Internet-conferencing, social-business, social-networking, voip-video, and web-posting. Whereas, subcategories in the business-systems category include auth-service, database, erp-crm, general-business, management, office-programs, software-update, and storage-backup.
Technology	The application technology will be one of the following: • client-server: An application that uses a client-server model where one or more clients communicate with a server in the network.

Application Details	Description
	• network-protocol: An application that is generally used for system-to-system communication that facilitates network operation. This includes most of the IP protocols. • peer-to-peer: An application that communicates directly with other clients to transfer information instead of relying on a central server to facilitate the communication. • browser-based: An application that relies on a web browser to function.
Risk	Assigned risk of the application. To customize this setting, click the **Customize** link, enter a value (1-5), and click **OK**.
Tags	Tags assigned to an application. **Edit Tags** to add or remove tags for an application.
Options	
Session Timeout	Period of time, in seconds, required for the application to time out due to inactivity (range is 1-604800 seconds). This timeout is for protocols other than TCP or UDP. For TCP and UDP, refer to the next rows in this table. To customize this setting, click the **Customize** link, enter a value, and click **OK**.
TCP Timeout (seconds)	Timeout, in seconds, for terminating a TCP application flow (range is 1-604800). To customize this setting, click the **Customize** link, enter a value, and click **OK**. A value of 0 indicates that the global session timer will be used, which is 3600 seconds for TCP.
UDP Timeout (seconds):	Timeout, in seconds, for terminating a UDP application flow (range is 1-604800 seconds). To customize this setting, click the **Customize** link, enter a value, and click **OK**.
TCP Half Closed (seconds)	Maximum length of time, in seconds, that a session remains in the session table between receiving the first FIN packet and receiving the second FIN packet or RST packet. If the timer expires, the session is closed (range is 1-604800). Default: If this timer is not configured at the application level, the global setting is used. If this value is configured at the application level, it overrides the global **TCP Half Closed** setting.

Application Details	Description
TCP Time Wait (seconds)	Maximum length of time, in seconds, that a session remains in the session table after receiving the second FIN packet or a RST packet. If the timer expires, the session is closed (range is 1-600). Default: If this timer is not configured at the application level, the global setting is used. If this value is configured at the application level, it overrides the global **TCP Time Wait** setting.
App-ID Enabled	Indicates whether the App-ID is enabled or disabled. If an App-ID is disabled, traffic for that application will be treated as the **Previously Identified As** App-ID in both Security policy and in logs. For applications added after content release version 490, you have the ability to disable them while you review the policy impact of the new app. After reviewing policy, you may choose to **enable** the App-ID. You also have the ability to **disable** an application that you have previously enabled. On a multi-vsys firewall, you can disable App-IDs separately in each virtual system.

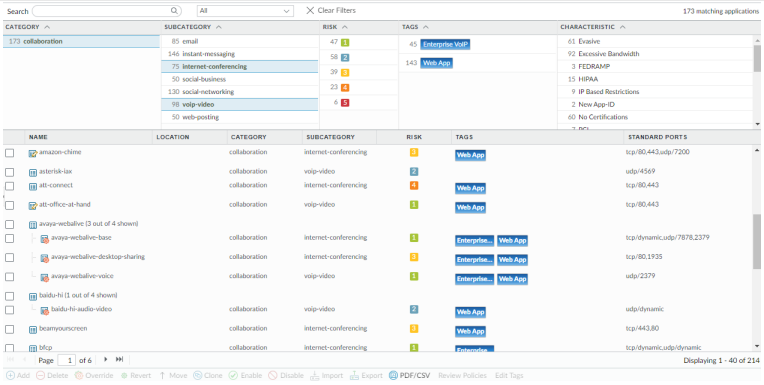
When the firewall is not able to identify an application using the App-ID, the traffic is classified as unknown: unknown-tcp or unknown-udp. This behavior applies to all unknown applications except those that fully emulate HTTP. For more information, refer to Monitor > Botnet.

You can create new definitions for unknown applications and then define security policies for the new application definitions. In addition, applications that require the same security settings can be combined into application groups to simplify the creation of security policies.

Actions Supported on Applications

You can perform any of the following actions on this page:

Actions Supported for Applications	Description
Filter by application	• To search for a specific application, enter the application name or description in the **Search** field and press **Enter**. The drop-down allows you to search or filter for a specific application or view **All** applications, **Custom applications**, **Disabled applications**, or **Tagged applications**. The application is listed and the filter columns are updated to show statistics for the applications that matched the search. A search will match partial strings. When you define security policies, you can write rules that apply to all applications that match a saved filter. Such rules are dynamically updated when a new application is added through a content update that matches the filter. • To filter by application attributes displayed on the page, click an item to use as a basis for filtering. For example, to restrict the list to the collaboration category, click **collaboration** and the list will display only applications in this category.

Actions Supported for Applications	Description
	 • To filter on additional columns, select an entry in the other columns. The filtering is successive: Category filters are applied first, then Subcategory filters, then Technology filters, then Risk filters, and finally Characteristic filters. For example, if you apply a Category, Subcategory, and Risk filter, the Technology column is automatically restricted to the technologies that are consistent with the selected Category and Subcategory even though a Technology filter is not explicitly applied. Each time you apply a filter, the list of applications automatically updates. To create a new application filter, see Objects > Application Filters.
Add a new application.	To add a new application, see Defining Applications.
View and/or customize application details.	Click the application name link, to view the application description including the standard port and characteristics of the application, risk among other details. For details on the application settings, see Defining Applications. If the icon to the left of the application name has a yellow pencil ( ), the application is a custom application.
Disable an applications	You can **Disable** an application (or several applications) so that the application signature is not matched against traffic. Security rules defined to block, allow, or enforce a matching application are not applied to the application traffic when the app is disabled. You might choose to disable an application that is included with a new content release version because policy enforcement for the application might change when the application is uniquely identified. For example, an application that is identified as web-browsing traffic is allowed by the firewall prior to a new content version installation; after installing the content update, the uniquely identified application no longer matches the Security rule that allows web-browsing traffic. In this case, you could choose to disable the application so that traffic matched to the application signature continues to be classified as web-browsing traffic and is allowed.
Enable an application	Select a disabled application and **Enable** it so that the firewall can manage the application according to your configured security policies.

Actions Supported for Applications	Description
Import an application	To import an application, click **Import**. Browse to select the file, and select the target virtual system from the **Destination** drop-down.
Export an application	To export an application, select this option for the application and click **Export**. Follow the prompts to save the file.
Export an application configuration table	Export the information on all applications in **PDF/CSV** format. Only visible columns in the web interface are exported. See Export Configuration Table Data.
Assess policy impact after installing a new content release	**Review Policies** to assess the policy-based enforcement for applications before and after installing a content release version. Use the Policy Review dialog to review policy impact for new applications included in a downloaded content release version. The Policy Review dialog allows you to add or remove a pending application (an application that is downloaded with a content release version but is not installed on the firewall) to or from an existing Security policy rule; policy changes for pending applications do not take effect until the corresponding content release version is installed. You can also access the Policy Review dialog when downloading and installing content release versions on the **Device** > **Dynamic Updates** page.
Tag an application	A predefined tag named **sanctioned** is available for you to tag SaaS applications. While a SaaS application is an application that is identified as **Saas=yes** in the details on application characteristics, you can use the sanctioned tag on any application. *Tag applications as sanctioned to help differentiate sanctioned SaaS application traffic from unsanctioned SaaS application traffic, for example, when you examine the SaaS Application Usage Report or when you evaluate the applications on your network.* Select an application, click **Edit Tags** and from the drop-down, select the predefined **Sanctioned** tag to identify any application that you want to explicitly allow on your network. When you then generate the SaaS Application Usage Report (see Monitor > PDF Reports > SaaS Application Usage), you can compare statistics on the application that you have sanctioned versus unsanctioned SaaS applications that are being used on your network. When you tag an application as sanctioned, the following restrictions apply: • The sanctioned tag cannot be applied to an application group. • The sanctioned tag cannot be applied at the **Shared** level; you can tag an application only per device group or per virtual system. • The sanctioned tag cannot be used to tag applications included in a container app, such as facebook-mail, which is part of the facebook container app.

Actions Supported for Applications	Description
	You can also **Remove tag** or **Override tag**. The override option is only available on a firewall that has inherited settings from a device group pushed from Panorama.

Defining Applications

Select **Objects** > **Applications** to **Add** a new custom application for the firewall to evaluate when applying policies.

New Application Settings	Description
Configuration Tab	
Name	Enter the application name (up to 31 characters). This name appears in the applications list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, periods, hyphens, and underscores. The first character must be a letter.
Shared	Select this option if you want the application to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the application will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the application will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this application object in device groups that inherit the object. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Description	Enter a description of the application for general reference (up to 255 characters).
Category	Select the application category, such as **email** or **database**. The category is used to generate the Top Ten Application Categories chart and is available for filtering (refer to ACC).
Subcategory	Select the application subcategory, such as **email** or **database**. The subcategory is used to generate the Top Ten Application Categories chart and is available for filtering (refer to ACC).
Technology	Select the technology for the application.
Parent App	Specify a parent application for this application. This setting applies when a session matches both the parent and the custom applications; however, the custom application is reported because it is more specific.

New Application Settings	Description
Risk	Select the risk level associated with this application (1=lowest to 5=highest).
Characteristics	Select the application characteristics that may place the application at risk. For a description of each characteristic, refer to Characteristics.
Advanced Tab	
Port	If the protocol used by the application is TCP and/or UDP, select **Port** and enter one or more combinations of the protocol and port number (one entry per line). The general format is: *<protocol>/<port>* where the *<port>* is a single port number, or **dynamic** for dynamic port assignment. Examples: TCP/dynamic or UDP/32. This setting applies when using **app-default** in the Service column of a Security rule.
IP Protocol	To specify an IP protocol other than TCP or UDP, select **IP Protocol**, and enter the protocol number (1 to 255).
ICMP Type	To specify an Internet Control Message Protocol version 4 (ICMP) type, select **ICMP Type** and enter the type number (range is 0-255).
ICMP6 Type	To specify an Internet Control Message Protocol version 6 (ICMPv6) type, select **ICMP6 Type** and enter the type number (range is 0-255).
None	To specify signatures independent of protocol, select **None**.
Timeout	Enter the number of seconds before an idle application flow is terminated (range is 0-604800 seconds). A zero indicates that the default timeout of the application will be used. This value is used for protocols other than TCP and UDP in all cases and for TCP and UDP timeouts when the TCP timeout and UDP timeout are not specified.
TCP Timeout	Enter the number of seconds before an idle TCP application flow is terminated (range is 0-604800 seconds). A zero indicates that the default timeout of the application will be used.
UDP Timeout	Enter the number of seconds before an idle UDP application flow is terminated (range is 0-604800 seconds). A zero indicates that the default timeout of the application will be used.
TCP Half Closed	Enter the maximum length of time that a session remains in the session table, between receiving the first FIN and receiving the second FIN or RST. If the timer expires, the session is closed. Default: If this timer is not configured at the application level, the global setting is used (range is 1-604800 seconds).

New Application Settings	Description
	If this value is configured at the application level, it overrides the global TCP Half Closed setting.
TCP Time Wait	Enter the maximum length of time that a session remains in the session table after receiving the second FIN or a RST. If the timer expires, the session is closed. Default: If this timer is not configured at the application level, the global setting is used (range is 1-600 seconds). If this value is configured at the application level, it overrides the global TCP Time Wait setting.
Scanning	Select the scanning types that you want to allow based on Security Profiles (file types, data patterns, and viruses).
Signatures Tab	
Signatures	Click **Add** to add a new signature, and specify the following information: • **Signature Name**—Enter a name to identify the signature. • **Comment**—Enter an optional description. • **Ordered Condition Match**—Select if the order in which signature conditions are defined is important. • **Scope**—Select whether to apply this signature only to the current **Transaction** or to the full user **Session**. Specify the conditions that identify the signature. These conditions are used to generate the signature that the firewall uses to match the application patterns and control traffic: • To add a condition, select **Add And Condition** or **Add Or Condition**. To add a condition within a group, select the group and then click **Add Condition**. • Select an **Operator** from the drop-down. The options are **Pattern Match**, **Greater Than**, **Less Than**, and **Equal To** and specify the following options: (For Pattern Match only) • **Context**—Select from the available contexts. These contexts are updated using dynamic content updates. • **Pattern**— Specify a regular expression to specify unique string context values that apply to the custom application. *Perform a packet capture to identify the context. See Pattern Rules Syntax for pattern rules for regular expressions.* (For Greater Than, Less Than) • **Context**—Select from the available contexts. These contexts are updated using dynamic content updates • **Value**—Specify a value to match on (range is 0-4294967295). • **Qualifier and Value**—(Optional) Add qualifier/value pairs. (For Equal To only)

New Application Settings	Description
	• **Context**—Select from unknown requests and responses for TCP or UDP (for example, unknown-req-tcp) or additional contexts that are available through dynamic content updates (for example, dnp3-req-func-code). For unknown requests and responses for TCP or UDP, specify • **Position**—Select between the first four or second four bytes in the payload. • **Mask**—Specify a 4-byte hex value, for example, 0xffffff00. • **Value**—Specify a 4-byte hex value, for example, 0xaabbccdd. For all other contexts, specify a **Value** that is pertinent to the application. To move a condition within a group, select the condition and **Move Up** or **Move Down**. To move a group, select the group and **Move Up** or **Move Down**. You cannot move conditions from one group to another.

It is not required to specify signatures for the application if the application is used only for application override rules.

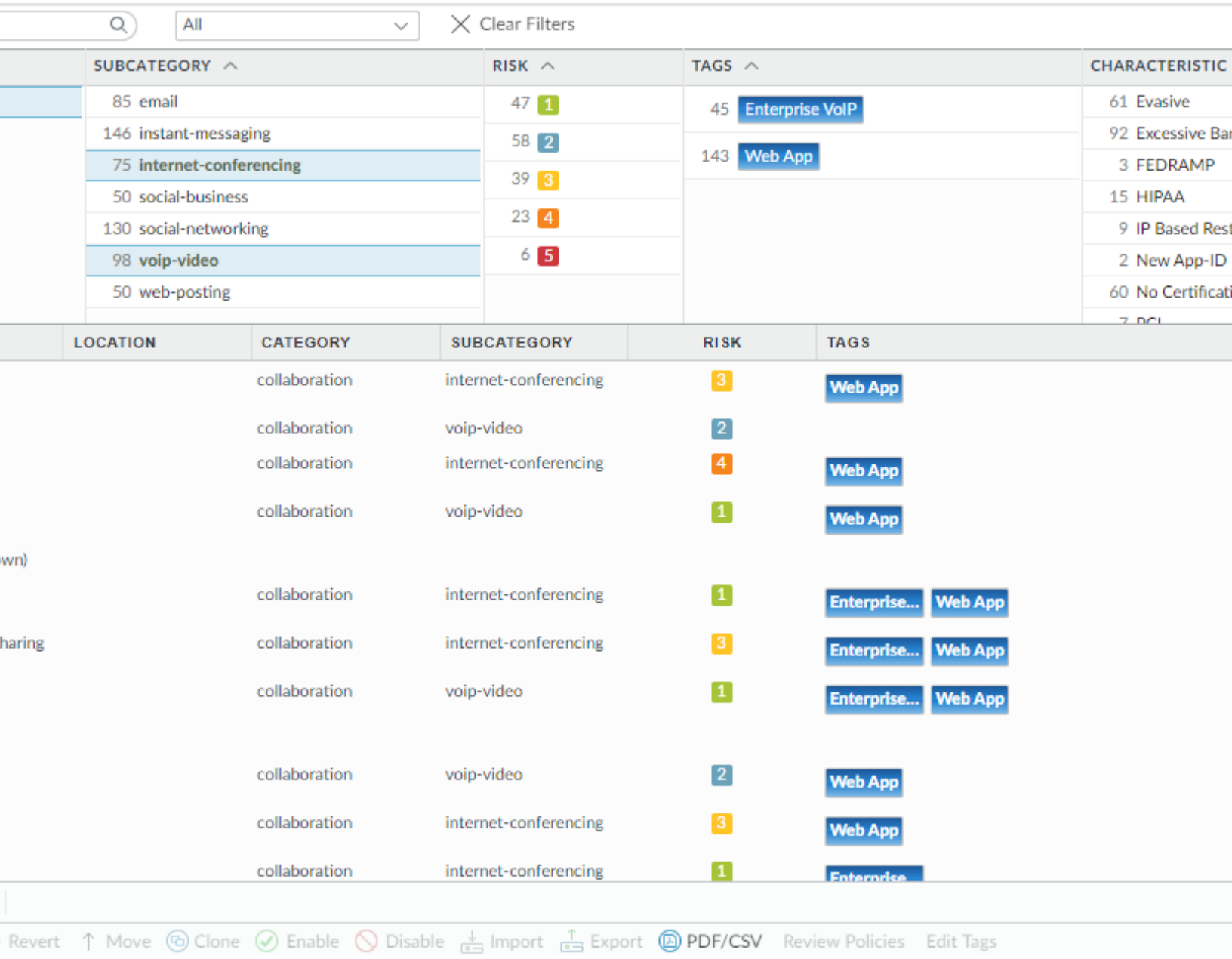
Objects > Application Groups

To simplify the creation of security policies, applications requiring the same security settings can be combined by creating an application group. (To define a new application, refer to Defining Applications.)

New Application Group Settings	Description
Name	Enter a name that describes the application group (up to 31 characters). This name appears in the application list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this option if you want the application group to be available to: Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the application group will be available only to the **Virtual System** selected in the **Objects** tab. Every device group on Panorama. If you clear this selection, the application group will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this application group object in device groups that inherit the object. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Applications	Click **Add** and select applications, application filters, and/or other application groups to be included in this group.

Objects > Application Filters

Application filters help to simplify repeated searches. To define an application filter, **Add** and enter a name for your new filter. In the upper area of the window, click an item that you want to use as a basis for filtering. For example, to restrict the list to the Collaboration category, click **collaboration**.



To filter on additional columns, select an entry in the columns. The filtering is successive: category filters are applied first followed by subcategory filters, technology filters, risk filters, tags, and then characteristic filters.

As you select filters, the list of applications that display on the page is automatically updated.

Objects > Services

When you define security policies for specific applications, you can select one or more services to limit the port numbers the applications can use. The default service is **any**, which allows all TCP and UDP ports. The HTTP and HTTPS services are predefined, but you can add additional service definitions. Services that are often assigned together can be combined into service groups to simplify the creation of security policies (refer to Objects>ServiceGroups).

Additionally, you can use service objects to specify service-based session timeouts—this means that you can apply different timeouts to different user groups even when those groups are using the same TCP or UDP service, or, if you're migrating from an port-based security policy with custom applications to an application-based security policy, you can easily maintain your custom application timeouts.

The following table describes the service settings:

Service Settings	Description
Name	Enter the service name (up to **63** characters). This name appears in the services list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the service (up to 1023 characters).
Shared	Select this option if you want the service object to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the service object will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the service object will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this service object in device groups that inherit the object. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Protocol	Select the protocol used by the service (**TCP** or **UDP**).
Destination Port	Enter the destination port number (0 to 65535) or range of port numbers (port1-port2) used by the service. Multiple ports or ranges must be separated by commas. The destination port is required.
Source Port	Enter the source port number (0 to 65535) or range of port numbers (port1-port2) used by the service. Multiple ports or ranges must be separated by commas. The source port is optional.
Session Timeout	Define the session timeout for the service: • **Inherit from application** (default)—No service-based timeouts are applied; the application timeout is applied.

Service Settings	Description
	• **Override**—Define a custom session timeout for the service. Continue to populate the TCP Timeout, TCP Half Closed, and TCP Wait Time fields.
The following settings display only if you choose to override application timeouts and create custom session timeouts for a service:	
TCP Timeout	Set the maximum length of time in seconds that a TCP session can remain open after data transmission has started. When this time expires, the session closes. Range is 1 - 604800. Default value is 3600 seconds.
TCP Half Closed	Set the maximum length of time in seconds that a session remains open when only one side of the connection has attempted to close the connection. This setting applies to: • The time period after the firewall receives the first FIN packet (indicates that one side of the connection is attempting to close the session) but before it receives the second FIN packet (indicates that the other side of the connection is closing the session). • The time period before receiving an RST packet (indicating an attempt to reset the connection). If the timer expires, the session closes. Range is 1 - 604800. Default value is 120 seconds.
TCP Wait Time	Set the maximum length of time in seconds that a session remains open after receiving the second of the two FIN packets required to terminate a session, or after receiving an RST packet to reset a connection. When the timer expires, the session closes. Range is 1 - 600. Default value is 15 seconds.

Objects > Service Groups

To simplify the creation of security policies, you can combine services that have the same security settings into service groups. To define new services, refer to Objects > Services.

The following table describes the service group settings:

Service Group Settings	Description
Name	Enter the service group name (up to **63** characters). This name appears in the services list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this option if you want the service group to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the service group will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the service group will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this service group object in device groups that inherit the object. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Service	Click **Add** to add services to the group. Select from the drop-down or click **Service** at the bottom of the drop-down and specify the settings. Refer to Objects > Services for a description of the settings.

Objects > Tags

Tags allow you to group objects using keywords or phrases. You can apply tags to address objects, address groups (static and dynamic), applications, zones, services, service groups, and to policy rules. You can also use an SD-WAN Interface profile to apply a link tag to an Ethernet interface. You can use tags to sort or filter objects and to visually distinguish objects by color. When you apply a color to a tag, the **Policy** tab displays the object with a background color.

You must create a tag before you can group rules using that tag. After you assign grouped rules by a tag, **View Rulebase as Groups** to see a visual representation of your policy rulebase based on the assigned tags. While viewing your rulebase as groups, the policy order and priority is maintained. In this view, select the group tag to view all rules grouped by that tag.

A predefined tag named **Sanctioned** is available for tagging applications (**Objects** > **Applications**). These tags are required for accuracy (Monitor > PDF Reports > SaaS Application Usage).

What do you want to know?	See:
How do I create tags?	Create Tags
How do I view the rulebase as groups?	View Rulebase as Groups
Search for rules that are tagged. Group rules using tags. View tags used in policy. Apply tags to policy.	Manage Tags
Looking for more?	• Use Tags to Group and Visually Distinguish Objects • SD-WAN Link Tag

Create Tags

- **Objects** > **Tags**

Select **Tags** to create a tag, assign a color or to delete, rename, and clone tags. Each object can have up to 64 tags; when an object has multiple tags, it displays the color of the first tag applied.

On the firewall, the **Tags** tab displays the tags that you define locally on the firewall or push from Panorama to the firewall. On Panorama, the **Tags** tab displays the tags that you define on Panorama. This tab does not display the tags that are dynamically retrieved from the VM Information sources defined on the firewall for forming dynamic address groups nor does it display tags that are defined using the XML or REST API.

When you create a new tag, the tag is automatically created in the Virtual System or Device Group that is currently selected on the firewall or Panorama.

Tag Settings	Description
Name	Enter a unique tag name (up to 127 characters). The name is not case-sensitive.

Tag Settings	Description
Shared	Select this option if you want the tag to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the tag is available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you disable (clear) this option, the tag will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this tag in device groups that inherit the tag. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the tag.
Color	Select a color from the color palette in the drop-down (default is None).
Comments	Add a label or description to describe for what the tag is used.

- Add a tag: **Add** a tag and then fill in the following fields:

  You can also create a new tag when you create or edit policy in the **Policies** tab. The tag is automatically created in the Device Group or Virtual System that is currently selected.
- Edit a tag: Click a tag to edit, rename, or assign a color to a tag.
- Delete a tag: Click **Delete** and select the tag. You cannot delete a predefined tag.
- Move or Clone a tag: The options to move or clone a tag allow you to copy a tag or move a tag to a different Device Group or Virtual System on firewalls with multiple virtual systems enabled.

  Move or Clone and select the tag. Select the **Destination** location—Device Group or Virtual System. Disable (clear) this option to **Error out on first detected error in validation** if you want the validation process to discover all errors for the object before displaying the errors. This option is enabled by default and the validation process stops when the first error is detected and only displays the error.
- Override or Revert a tag (Panorama only): The **Override** option is available only if you did not select the **Disable override** option when you created the tag. The **Override** option allows you to override the color assigned to the tag that was inherited from a shared or ancestor device group. The **Location** is the current device group. You can also **Disable override** to prevent future override attempts.

  Revert changes to undo recent modifications of a tag. When you revert a tag, the **Location** field displays the device group or virtual system from where the tag was inherited.

View Rulebase as Groups

- **Policies** > **<Rulebase Type>**

View Rulebase as Groups to display the policy rulebase using the group tag. While viewing your rulebase as groups, the policy order and priority is maintained. In this view, select the group tag to view all rules grouped by that tag.

When viewing your rulebase as groups, click **Group** to move, change, delete, or clone all rules in the selected tag group. The following table describes the rule management options available when viewing your rulebase as groups.

Option	Description
Move Rules in Group to Different Rulebase or Device Group	Move all policy rules in the selected tag group to a different rulebase or device group.
Change Group of All Rules	Move all rules in the selected tag group to a different tag group.
Move All Rules in Group	Move all rules in the selected tag group within the rulebase.
Delete All Rules in Group	Delete all rules in the selected tag group.
Clone All Rules in Group	Clone all rules in the selected tag group.

Move Rules in Group to Different Rulebase or Device Group

If you need to organize your rulebase, select the tag group containing the rules you want to move and **Move Rules in Group to Different Rulesbase or Device Group** to reassign them to a different rulebase or device group (instead of moving each rule individually). The device group must already exist before (cannot be created while) moving rules in a tag group to a different device group. Additionally, you can move the rules in a tag group to a different rulebase within the same device group.

To move rules to a different rulebase or device group, enter the following:

Field	Description
Destination	The target device group to move the policy rules.
(Panorama only) Destination Type	Select whether to move the rules to the **Pre-Rulebase** or **Post-Rulebase** of the destination device group.
Rule Order	Select where in the rulebase to move the rules. You can choose: • **Move Top**—Move rules to the top of the rulebase of the destination device group. • **Move Bottom**—Move rules to the end of the rulebase of the destination device group. • **Before Rule**—Move rules before the selected rule in the rulebase of the destination device group. • **After Rule**—Move rules after the selected rule in the rulebase of the destination device group.
Error out on first detected error in validation	Check this box to determine how errors are displayed if encountered during validation. If checked, each error is displayed individually. If unchecked, the errors are aggregated and displayed as a single error. Errors detected during validation cause the rule move job to fail, and no rules are moved to the destination device group.

Change Group of All Rules

Rather than editing each rule, **Change Group of All Rules** to move an entire policy rule set from one tag group to another existing tag group. The rule order of the tag group rules is preserved when moved to the new tag group, but you have the choice of placing the new rules either before the rules in the destination tag group, or after.

To move rules to a different tag group, specify the destination tag group and whereto place the moved rules.

Field	Description
Select a Group for its appearance order	Select the destination tag group.
Move Top	**Move Top** inserts the rules at the top of the destination tag group.
Move Bottom	**Move bottom** inserts the rules at the bottom of the destination tag group.

Move All Rules in Group

Rather than reordering each rule individually, **Move All Rules in Group** to move all rules in the selected tag group up or down the rule hierarchy. The rule order of the moved rules in the tag group rules is preserved when moving the tag group, but you have the choice of placing the rules either before the rules in the destination tag group, or after.

To move rules, specify the destination tag group and where to place the moved rules.

Field	Description
Select a Group for its appearance order	Select the destination tag group.
Move Top	**Move Top** inserts the rules at before the destination tag group.
Move Bottom	**Move bottom** inserts the rules after the destination tag group.

Delete All Rules in Group

To simplify rule management, you can **Delete All Rules in Group** to reduce your security risks and keep your policy rulebase organized by deleting unused or unwanted rules associated with a selected tag group.

Clone All Rules in Group

Rather than manually recreate existing policy rules in a tag group, **Clone All Rules in Group** to quickly duplicate rules in the selected tag group in the device group and rulebase of your choice. The device group must already exist before (cannot be created while) cloning rules in a tag group to a different device group. Additionally, you can clone the rules in a tag group to a different rulebase within the same device group.

Cloned rules are appended with the rule name and the following format: `<Rule Name>-1`. If a rule is cloned to the same location as the first cloned rule, and the name is not changed, then the name is appended. For example, `<Rule Name>-2`, `<Rule Name>-3`, and so on.

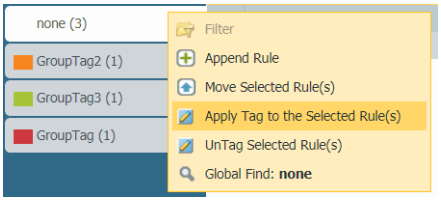
To clone rules, configure the following fields.

Field	Description
Destination	The target device group of the cloned policy rules.
(Panorama only) Destination Type	Select whether to clone the rules to the **Pre-Rulebase** or **Post-Rulebase** of the destination device group.
Rule Order	Select where in the rulebase to clone the rules. You can choose: • **Move Top**—Insert cloned rules at the top of the rulebase of the destination device group. • **Move Bottom**—Insert cloned rules at the end of the rulebase of the destination device group. • **Before Rule**—Insert cloned rules before the selected rule in the rulebase of the destination device group. • **After Rule**—Inserted cloned rules after the selected rule in the rulebase of the destination device group.
Error out on first detected error in validation	Select this option to determine how errors are displayed if encountered during validation. If enabled, each error is displayed individually. If disabled (cleared), the errors are aggregated and displayed as a single error. Errors detected during validation cause the rule clone job to fail, and no rules are cloned to the destination device group.

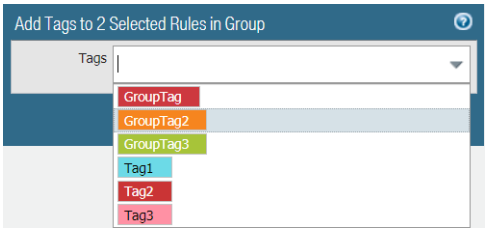
Manage Tags

The following table lists the actions that you can perform when grouping rules by group tags.

- Tag a rule.
  1. Select **View Rules as Groups**.
  2. Select one or more rules on the right pane.
  3. From the group tag drop-down, **Apply Tag to the Selected Rules**.



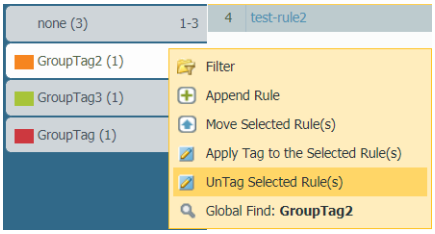
  4. Add tags to the selected rules.



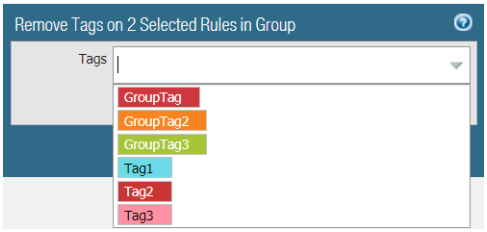
- View the rules assigned a group tag.
  1. **View Rulebase as Groups** to view the group tags your rules are assigned to.
  2. The right pane updates to display the group tags. rules that have any of the selected tags.

3. Select the group tag to view the rules assigned to the group. Rules not assigned a group tag are listed in the **none** group.

- Untag a rule.
  1. **View Rulebase as Groups** to view the group tags your rules are assigned to.
  2. Select one or more rules on the right pane.
  3. From the group tag drop-down, **Apply Tag to the Selected Rules**.

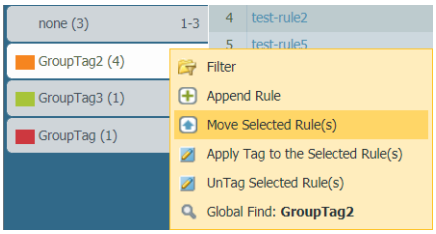


  4. Remove tags to the selected rules. Additionally, you may **Delete All** tags assigned to the rule.



- Reorder a rule using tags.

  When you **View Rulebase as Groups**, select one or more rules in a group tag, hover over the rule number and select **Move Selected Rule(s)** in the drop-down. Do not select any rules if you want to move all rules in the selected group tag.



  Select a group tag from the drop-down in the move rule window and select whether you want to **Move Before** or **Move After** the tag selected in the drop-down.

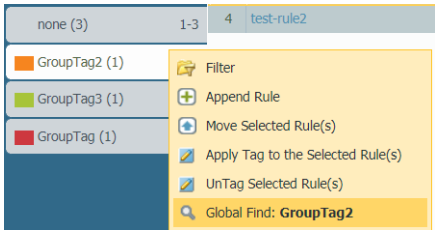
- Add a new rule that applies the selected tags.

  When you **View Rulebase as Groups**, hover over the group tag and select **Append Rule** in the drop-down.

  The new rule is appended to the end of the list of rules assigned to the group tag.

- Search for a group tag.

  When you **View Rulebase as Groups**, hover over the group tag and from the drop-down select **Global Find**.



- Export tag configuration table.

  Administrative roles can export the object configuration table in **PDF/CSV** format and can apply filters to customize the table output to include only the columns you need. Only the columns that are visible in the Export dialogue exported. See Export Configuration Table Data.

Objects > Devices

Also known as the Device Dictionary, this page contains metadata for device objects. Review information for existing device objects or add a new device objects. Using device objects as match criteria in security policy allows you to create device-based policy, where the firewall dynamically updates and applies security policy to new and existing devices. Palo Alto Networks updates the Device Dictionary via dynamic updates, which you can view in **Device** > **Dynamic Updates** > **Device-ID Content**.

Button/Field	Description
Name	The name of the device object.
Location	The location of the device group for the device object.
Category	The category of the device object (for example, `Video Audio Conference`).
Profile	The device profile for the device object.
Model	The model of the device object.
OS Version	The OS version of the device object.
OS Family	The OS family of the device object.
Vendor	The vendor for the device object.
Add	Click **Add** to add a new device object. Enter a **Name** and optionally, a **Description**. Select additional metadata for the device, such as **Category**, **OS**, and **Model**. You can also **Browse** the list of devices to select the device you want to add. Click **OK** to confirm your changes.
Delete	Select a device object you no longer need then **Delete** it.
Move	Select the device object you want to move then **Move** it.
Clone	Select the device object on which to base the new device profile and **Clone** it.
PDF/CSV	Export the list of devices in **PDF/CSV** format. You can apply filters to create more specific outputs as needed. Only visible columns in the web interface will be exported. See Configuration Table Export.

Objects > External Dynamic Lists

An external dynamic list is an address object based on an imported list of IP addresses, URLs, domain names, International Mobile Equipment Identities (IMEIs), or International Mobile Subscriber Identities (IMSIs) that you can use in policy rules to block or allow traffic. This list must be a text file saved to a web server that is accessible by the firewall. By default, the firewall uses the management (MGT) interface to retrieve this list.

With an active Threat Prevention license, Palo Alto Networks provides multiple built-in dynamic IP lists that you can use to block malicious hosts. We update the lists daily based on our latest threat research.

You can use an IP address list as an address object in the source and destination of your policy rules; you can use a URL List in a URL Filtering profile (Objects > Security Profiles > URL Filtering) or as a match criteria in Security policy rules; and you can use a domain list (Objects > Security Profiles > Anti-Spyware Profile) as a sinkhole for specified domain names.

On each firewall model, you can use up to 30 external dynamic lists with unique sources across all Security policy rules. The maximum number of entries that the firewall supports for each list type varies based on the firewall model (refer to the different firewall limits for each external dynamic list type). List entries count toward the maximum limit only if the external dynamic list is used in a policy rule. If you exceed the maximum number of entries that are supported on a firewall model, the firewall generates a System log and skips the entries that exceed the limit. To check the number of IP addresses, domains, URLs, IMEIs, and IMSIs currently used in policy rules and the total number supported on the firewall, select **List Capacities** (firewall only).

The external dynamic lists are shown in the order they are evaluated from top to bottom. Use the directional controls at the bottom of the page to change the list order. This enables you to reorder the lists to make sure that the most important entries in an external dynamic list are committed before you reach capacity limits.

You cannot change the external dynamic list order when lists are grouped by type.

To retrieve the latest version of the external dynamic list from the server that hosts it, select an external dynamic list and **Import Now**.

You cannot delete, clone, or edit the settings of the Palo Alto Networks malicious IP address feeds.

Add a new external dynamic list and configure the settings described in the table below.

External Dynamic List Settings	Description
Name	Enter a name to identify the external dynamic list (up to 32 characters). This name identifies the list for policy rule enforcement.
Shared (Multiple virtual systems (multi-vsys) and Panorama only)	Enable this option if you want the external dynamic list to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you disable (clear) this option, then the external dynamic list is available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama.

External Dynamic List Settings	Description
	If you disable (clear) this option, the external dynamic list is available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Enable this option to prevent administrators from overriding the settings of this external dynamic list object in device groups that inherit the object. This option is disabled (cleared) by default, which means administrators can override the settings for any device group that inherits the object.
Test Source URL (Firewall only)	**Test Source URL** to verify that the firewall can connect to the server that hosts the external dynamic list.  *This test does not check whether the server authenticates successfully.*
Create List Tab	

Type
  *You cannot mix IP addresses, URLs, and domain names in a single list. Each list must include entries of only one type.*
	Select from the following types of external dynamic lists:
	• **Predefined IP List**—Use a list that Palo Alto Networks identifies as bulletproof IP addresses, known malicious IP addresses, or high risk IP addresses as a source of list entries (requires an active Threat Prevention license).
	• **Predefined URL List**—Use a list of domains that Palo Alto Networks identifies as trusted to exclude these domains from Authentication policy.
	• **IP List** (default)—Each list can include IPv4 or IPv6 addresses, address ranges, and subnets. The list must contain only one IP address, range, or subnet per line. For example:
	`192.168.80.150/32`
	`2001:db8:123:1::1 or 2001:db8:123:1::/64`
	`192.168.80.0/24`
	`2001:db8:123:1::1 - 2001:db8:123:1::22`
	In the example above, the first line indicates all addresses from 192.168.80.0 through 192.168.80.255. A subnet or an IP address range, such as 92.168.20.0/24 or 192.168.20.40 – 192.168.20.50, counts as one IP address entry and not as multiple IP addresses.
	• **Domain List**—Each list can contain only one domain name entry per line. For example:
	`www.p301srv03.paloalonetworks.com`
	`ftp.example.co.uk`
	`test.domain.net`
	For the list of domains included in the external dynamic list, the firewall creates a set of custom signatures of the spyware type with medium severity so that you can use the sinkhole action for a custom list of domains.

External Dynamic List Settings	Description

	• **URL List**—Each list can have only one URL entry per line. For example:
	
	`financialtimes.co.in`
	`www.wallaby.au/joey`
	`www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx`
	`*.example.com/*`
	
	For each URL list, the default action is set to **Allow**. To edit the default action, see Objects > Security Profiles > URL Filtering.

Type (cont)	• **Subscriber Identity List**—Each list contains subscriber IDs for a 3G, 4G, or 5G network. In the Source field, enter a URL for the firewall to access the list. • **Equipment Identity List**—Each list contains equipment IDs for a 3G, 4G, or 5G network. In the Source field, enter a URL for the firewall to access the list. *Determine which firewall model to purchase based on the total number of 3G, 4G, and 5G network identifiers you need your dynamic external dynamic list and static entries to support.*
Description	Enter a description for the external dynamic list (up to 255 characters).
Source	• If the external dynamic list is a Predefined IP List, select **Palo Alto Networks - Bulletproof IP addresses**, **Palo Alto Networks - High risk IP addresses**, or **Palo Alto Networks - Known malicious IP addresses** as the list source. • If the external dynamic list is a Predefined URL List, the default setting is **panw-auth-portal-exclude-list**. • If the external dynamic list is an IP List, a Domain List, or a URL List, enter an HTTP or HTTPS URL path that contains the text file (for example, **`http://192.0.2.20/myfile.txt`**). • If the external dynamic list is a Domain List, the default setting is to **Automatically expand to include subdomains**. This option enables the PAN-OS® software to evaluate all lower-level components of the domain names listed in the external dynamic list file. • If the external dynamic list is a Subscriber Identity List or Equipment Identity List, enter a URL path that contains the list. *If your external dynamic list contains subdomains, these expanded entries count towards your appliance model capacity count. You can disable this feature if you want to manually define subdomains. However, subdomains that are not explicitly defined in the list are not evaluated by policy rules.*
Certificate Profile	If the external dynamic list has an HTTPS URL, select an existing certificate profile (firewall and Panorama) or create a new **Certificate**

External Dynamic List Settings	Description
(IP List, Domain List, or URL List only)	**Profile** (firewall only) for authenticating the web server that hosts the list. For more information on configuring a certificate profile, see Device > Certificate Management > Certificate Profile. Default: **None (Disable Cert profile)**  *To maximize the number of external dynamic lists that you can use to enforce policy, use the same certificate profile to authenticate external dynamic lists that use the same source URL so that the lists count as only one external dynamic list. External dynamic lists from the same source URL that use different certificate profiles are counted as unique external dynamic lists.*
Client Authentication	Enable this option (disabled by default) to add a username and password that the firewall will use when accessing an external dynamic list source that requires basic HTTP authentication. This setting is available only when the external dynamic list has an HTTPS URL. • **Username**—Enter a valid username to access the list. • **Password/Confirm Password**—Enter and confirm the password for the username.
Check for updates	Specify the frequency at which the firewall retrieves the list from the web server. You can set the interval to every **Every Five Minutes** (default), **Hourly**, **Daily**, **Weekly**, or **Monthly**, at which the firewall retrieves the list. The interval is relative to the last commit. So, for the five-minute interval, the commit occurs in 5 minutes if the last commit was an hour ago. The commit updates all policy rules that reference the list so that the firewall can successfully enforce policy rules.  *You do not have to configure a frequency for a predefined IP list because the firewall dynamically receives content updates with an active Threat Prevention license.*
List Entries and Exceptions Tab	
List Entries	Displays the entries in the external dynamic list. • **Add an entry as a list exception**—Select up to 100 entries and **Submit** (→). • **View an AutoFocus threat intelligence summary for an item**—Hover over an entry and select **AutoFocus** from the drop-down. You must have an AutoFocus™ license and enable AutoFocus threat intelligence to view an item summary (select **Device** > **Setup** > **Management** and edit the **AutoFocus** settings). • **Check if an IP address, domain, or URL is in the external dynamic list**—Enter a value in the filter field and **Apply Filter** (→). **Clear Filter** (**[X]**) to go back to viewing the complete list.
Manual Exceptions	Displays exceptions to the external dynamic list.

External Dynamic List Settings	Description
	• **Edit an exception**—Select an exception and make your changes. • **Manually enter an exception**—**Add** a new exception manually. • **Remove an exception from the Manual Exceptions list**—Select and **Delete** an exception. • **Check if an IP address, domain, or URL is in the Manual Exceptions list**—Enter a value in the filter field and **Apply Filter** (→). **Clear Filter** (**[X]**) to go back to viewing the complete list. You cannot save your changes to the external dynamic list if you have duplicate entries in the Manual Exceptions list.

Objects > Custom Objects

Create custom data patterns, vulnerability and spyware signatures, and URL categories to use with policies:

- Objects > Custom Objects > Data Patterns
- Objects > Custom Objects > Spyware/Vulnerability
- Objects > Custom Objects > URL Category

Objects > Custom Objects > Data Patterns

The following topics describe data patterns.

What are you looking for?	See:
Create a data pattern.	Data Pattern Settings
Learn more about syntax for regular expression data patterns and see some examples.	Syntax for Regular Expression Data Patterns Regular Expression Data Pattern Examples

Data Pattern Settings

Select **Objects** > **Custom Objects** > **Data Patterns** to define the categories of sensitive information that you may want to filter. For information on defining data filtering profiles, select Objects > Security Profiles > Data Filtering.

You can create three types of data patterns for the firewall to use when scanning for sensitive information:

- **Predefined**—Use the predefined data patterns to scan files for social security and credit card numbers.
- **Regular Expression**—Create custom data patterns using regular expressions.
- **File Properties**—Scan files for specific file properties and values.

Data Pattern Settings	Description
Name	Enter the data pattern name (up to 31 characters). The name case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the data pattern (up to 255 characters).
Shared	Select this option if you want the data pattern to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the data pattern will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the data pattern will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this data pattern object in device groups that inherit the object. This

Data Pattern Settings	Description
	selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Pattern Type	Select the type of data pattern you want to create: • Predefined Pattern • Regular Expression • File Properties
Predefined Pattern	Palo Alto Networks provides predefined data patterns to scan for certain types of information in files, for example, for credit card numbers or social security numbers. To configure data filtering based on a predefined pattern, **Add** a pattern and select the following: • **Name**—Select a predefined pattern to use to filter for sensitive data. When you pick a predefined pattern, the **Description** populates automatically. • Select the **File Type** in which you want to detect the predefined pattern.
Regular Expression	**Add** a custom data pattern. Give the pattern a descriptive **Name**, set the **File Type** you want to scan for the data pattern, and enter the regular expression that defines the **Data Pattern**. For regular expression data pattern syntax details and examples, see: • Syntax for Regular Expression Data Patterns • Regular Expression Data Pattern Examples
File Properties	Build a data pattern to scan for file properties and the associated values. For example, **Add** a data pattern to filter for Microsoft Word documents and PDFs where the document title includes the words “sensitive”, “internal”, or “confidential”. • Give the data pattern a descriptive **Name**. • Select the **File Type** that you want to scan. • Select the **File Property** that you want to scan for a specific value. • Enter the **Property Value** for which you want to scan.

Syntax for Regular Expression Data Patterns

The general pattern requirements and syntax for creating data patterns depends on the pattern-matching engine that you enable: classic or enhanced (default).

Pattern Requirements	Classic	Enhanced
Pattern length	Requires 7 literal characters, which cannot include a period (`.`), an asterisk (`*`), a plus sign (+), or a range (`[a-z]`).	Requires two literal characters.
Case-insensitivity	Requires you to define patterns for all possible strings to match all variations of a term.	Allows you to use the **`i`** option on a sub-pattern.

Pattern Requirements	Classic	Enhanced
	Example: To match any documents designated as confidential, you must create a pattern that includes “confidential,” “Confidential,” and “CONFIDENTIAL.”	Example: **`((?i)\bconfidential \b)`** matches `ConfiDential`

The regular expression syntax in PAN-OS® is similar to traditional regular expression engines but every engine is unique. The Classic Syntax and Enhanced Syntax tables describe the syntax supported in the PAN-OS pattern-matching engines.

Classic Syntax

Pattern Syntax	Description
.	Match any single character.
?	Match the preceding character or expression 0 or one time. You must include the general expression inside parentheses. Example: **`(abc)?`**
*	Match the preceding character or expression 0 or more times. You must include the general expression inside parentheses. Example: **`(abc)*`**
+	Match the preceding character or regular expression one or more times. You must include the general expression inside parentheses. Example: **`(abc)+`**
|	Specify one “OR” another. *You must include alternative substrings in parentheses.* Example: **`((bif)|(scr)|(exe))`** matches `bif`, `scr`, or `exe`.
-	Specify a range. Example: **`[c-z]`** matches any character between c and z inclusive.
[ ]	Match any specified character. Example: **`[abz]`** matches any of the specified characters—a, b, or z.
^	Match any character except those specified. Example: **`[^abz]`** matches any character except the specified characters—a, b, or z.
{ }	Match a string that contains minimum and maximum.

Pattern Syntax	Description
	Example: **{10-20}** matches any string that is between 10 and 20 bytes inclusive. You must specify this directly in front of a fixed string and you can use only a hyphen (**-**).
\	Perform a literal match on any character. You must precede the specified character with a backslash (\).
&amp	The ampersand (&) is a special character so, to look for & in a string, you must use **&amp**.

Enhanced Syntax

The enhanced pattern-matching engine supports all of the Classic Syntax as well as the following syntax:

Pattern Syntax	Description
Shorthand character classes Symbols that stand for a character of a specific type, such as a digit or white space. You can negate any of these shorthand character classes by using uppercase characters.	
\s	Match any whitespace character. Example: **\s** matches a space, tab, line break, or form feed.
\d	Match a character that is a digit [0-9]. Example: **\d** matches 0.
\w	Matches an ASCII character [A-Za-z0-9_]. Example: **\w\w\w** matches PAN.
\v	Match a vertical white space character, which includes all unicode line break characters. Example: **\v** matches a vertical white space character.
\h	Match horizontal white space, which includes the tab and all of the “space separator” unicode characters. Example: **\h** matches a horizontal white space character.
Bounded repeat quantifiers Specify how many times to repeat the previous item.	
{n}	Match exactly a number (*n*) of times. Example: **a{2}** matches aa.
{n,m}	**{n,m}** matches from *n* to *m* times.

Pattern Syntax	Description
	Example: **a{2,4}** matches aa, aaa, and aaaa
{n, }	**{n,}** matches at least *n* times. Example: **a{2,}** matches aaaaa in aaaaab.
Anchor characters Specify where to match an expression.	
^	Match at the beginning of a string. Also matches after every line break when multi-line mode (**m**) is enabled. Example: Given the string abc, **^a** matches a, but **^b** doesn't match anything because b doesn't occur at the start of the string.
$	Match at the end of a string or before a newline character at the end of a string. Also matches before every line break when multi-line mode (**m**) is enabled. Example: Given the string abc, **c$** matches c, but **a$** doesn't match anything because a doesn't occur at the end of the string.
\A	Match at the beginning of a string. Doesn't match after line breaks, even when multi-line mode (**m**) is enabled.
\Z	Match at the end of a string and before the final line break. Doesn't match before other line breaks even when multi-line mode (**m**) is enabled.
\z	Match at the absolute end of a string. Doesn't match before line breaks.
Option modifiers Change the behavior of a sub-pattern. Enter **(?<option>)** to enable or **(?-<option>)** to disable.	
i	Enable case-insensitivity. Example: **((?i)\bconfidential\b)** matches ConfiDential.
m	Make **^** and **$** match at the beginning and end of lines.
s	Make **.** match anything, including line break characters.
x	Ignore whitespace between regex tokens.

Regular Expression Data Pattern Examples

The following are examples of valid custom patterns:

- .*((Confidential)|(CONFIDENTIAL))

    - Looks for the word “Confidential” or “CONFIDENTIAL” anywhere
    - “.*” at the beginning specifies to look anywhere in the stream
    - Depending on the case-sensitivity requirements of the decoder, this may not match “confidential” (all lower case)
- .*((Proprietary &amp Confidential)|(Proprietary and Confidential))
    - Looks for either “Proprietary & Confidential” or “Proprietary and Confidential”
    - More precise than looking for “Confidential”
- .*(Press Release).*((Draft)|(DRAFT)|(draft))
    - Looks for “Press Release” followed by various forms of the word draft, which may indicate that the press release isn't ready to be sent outside the company
- .*(Trinidad)
    - Looks for a project code name, such as “Trinidad”

Objects > Custom Objects > Spyware/ Vulnerability

The firewall supports the ability to create custom spyware and vulnerability signatures using the firewall threat engine. You can write custom regular expression patterns to identify spyware phone home communication or vulnerability exploits. The resulting spyware and vulnerability patterns become available for use in any custom vulnerability profiles. The firewall looks for the custom-defined patterns in network traffic and takes the specified action for the vulnerability exploit.

Weekly content releases periodically include new decoders and contexts for which you can develop signatures.

You can optionally include a time attribute when defining custom signatures by specifying a threshold per interval for triggering possible actions in response to an attack. Action is taken only after the threshold is reached.

Use the **Custom Spyware Signature** page to define signatures for Anti-Spyware profiles. Use the **Custom Vulnerability Signature** page to define signatures for Vulnerability Protection profiles.

Custom Vulnerability and Spyware Signature Settings	Description
Configuration Tab	
Threat ID	Enter a numeric identifier for the configuration (spyware signatures range is 15000-18000 and 6900001 - 7000000; vulnerability signatures range is 41000-45000 and 6800001-6900000).
Name	Specify the threat name.
Shared	Select this option if you want the custom signature to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the custom signature will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the custom signature will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this signature in device groups that inherit the signature. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the signature.
Comment	Enter an optional comment.
Severity	Assign a level that indicates the seriousness of the threat.
Default Action	Assign the default action to take if the threat conditions are met. For a list of actions, see Actions in Security Profiles.

Custom Vulnerability and Spyware Signature Settings	Description
Direction	Indicate whether the threat is assessed from the client to server, server to client, or both.
Affected System	Indicate whether the threat involves the client, server, either, or both. Applies to vulnerability signatures, but not spyware signatures.
CVE	Specify the common vulnerability enumeration (CVE) as an external reference for additional background and analysis.
Vendor	Specify the vendor identifier for the vulnerability as an external reference for additional background and analysis.
Bugtraq	Specify the bugtraq (similar to CVE) as an external reference for additional background and analysis.
Reference	Add any links to additional analysis or background information. The information is shown when a user clicks on the threat from the ACC, logs, or vulnerability profile.
Signatures Tab	
Standard Signature	Select **Standard** and then **Add** a new signature. Specify the following information: • **Standard**—Enter a name to identify the signature. • **Comment**—Enter an optional description. • **Ordered Condition Match**—Select if the order in which signature conditions are defined is important. • **Scope**—Select whether to apply this signature only to the current transaction or to the full user session. Add a condition by clicking **Add Or Condition** or **Add And Condition**. To add a condition within a group, select the group and then click **Add Condition**. Add a condition to a signature so that the signature is generated for traffic when the parameters you define for the condition are true. Select an **Operator** from the drop-down. The operator defines the type of condition that must be true for the custom signature to match to traffic. Choose from **Less Than**, **Equal To**, **Greater Than**, or **Pattern Match** operators. • When choosing a **Pattern Match** operator, specify for the following to be true for the signature to match to traffic: • **Context**—Select from the available contexts. • **Pattern**—Specify a regular expression. See Pattern Rules Syntax for pattern rules for regular expressions. • **Qualifier and Value**—Optionally, add qualifier/value pairs. • **Negate**—Select **Negate** so that the custom signature matches to traffic only when the defined Pattern Match condition is not true. This allows you to ensure that the custom signature is not triggered under certain conditions.

Custom Vulnerability and Spyware Signature Settings	Description
	 *A custom signature cannot be created with only Negate conditions; at least one positive condition must be included in order for a negate condition to specified. Also, if the scope of the signature is set to Session, a Negate condition cannot be configured as the last condition to match to traffic.* You can define exceptions for custom vulnerability or spyware signatures using the new option to negate signature generation when traffic matches both a signature and the exception to the signature. Use this option to allow certain traffic in your network that might otherwise be classified as spyware or a vulnerability exploit. In this case, the signature is generated for traffic that matches the pattern; traffic that matches the pattern but also matches the exception to the pattern is excluded from signature generation and any associated policy action (such as being blocked or dropped). For example, you can define a signature to be generated for redirected URLs; however, you can now also create an exception where the signature is not generated for URLs that redirect to a trusted domain.
	• When choosing an **Equal To**, **Less Than**, or **Greater Than** operator, specify for the following to be true for the signature to match to traffic: • **Context**—Select from unknown requests and responses for TCP or UDP. • **Position**—Select between the first four or second four bytes in the payload. • **Mask**—Specify a 4-byte hex value, for example, 0xffffff00. • **Value**—Specify a 4-byte hex value, for example, 0xaabbccdd.
Combination Signature	Select **Combination** and specify the following information: Select **Combination Signatures** to specify conditions that define signatures: • Add a condition by clicking **Add AND Condition** or **Add OR Condition**. To add a condition within a group, select the group and then click **Add Condition**. • To move a condition within a group, select the condition and click **Move Up** or **Move Down**. To move a group, select the group and click **Move Up** or **Move Down**. You cannot move conditions from one group to another. Select **Time Attribute** to specify the following information: • **Number of Hits**—Specify the threshold that will trigger any policy-based action as a number of hits (1-1000) in a specified number of seconds (1-3600). • **Aggregation Criteria**—Specify whether the hits are tracked by source IP address, destination IP address, or a combination of source and destination IP addresses. • To move a condition within a group, select the condition and click **Move Up** or **Move Down**. To move a group, select the group and click **Move**

Custom Vulnerability and Spyware Signature Settings	Description
	Up or **Move Down**. You cannot move conditions from one group to another.

Objects > Custom Objects > URL Category

Use the custom URL category page to create your custom list of URLs and use it in a URL filtering profile or as match criteria in policy rules. In a custom URL category, you can add URL entries individually or you can import a text file that contains a list of URLs.

URL entries added to custom categories are case insensitive.

The following table describes the custom URL settings.

Custom URL Category Settings	Description
Name	Enter a name to identify the custom URL category (up to 31 characters). This name displays in the category list when defining URL filtering policies and in the match criteria for URL categories in policy rules. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the URL category (up to 255 characters).
Type	Select the category type: • **Category Match**—Select **Category Match** to define a new custom category containing URLs matching all of the specified URL categories (a URL has to match all categories in the list). Specify between 2-4 categories. • **URL List**—Select **URL List** to add or import a list of URLs for the category. This category type also contains URLs added before PAN-OS 9.0.
Shared	Select this option if you want the URL category to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you disable (clear) this option, the URL category is available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you disable (clear) this option, the URL category is available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this custom URL object in device groups that inherit the object. This selection is disabled by default, which means administrators can override the settings for any device group that inherits the object.
Sites	Manage sites for the custom URL category (each URL added or imported can have a maximum of 255 characters). • **Add**—**Add** URLs, only one per row. Each URL can be in the format “www.example.com” or can include wildcards, such as “*.example.com”. For additional information on supported formats, see Block List in Objects > Security Profiles > URL Filtering.

Custom URL Category Settings	Description
	• **Import**—**Import** and browse to select the text file that contains the list of URLs. Enter only one URL per row. Each URL can be in the format “www.example.com” or can include wildcards, such as “*.example.com”. For additional information on supported formats, see Block List in Objects > Security Profiles > URL Filtering. • **Export**—**Export** custom URL entries included in the list (exported as a text file). • **Delete**—**Delete** an entry to remove the URL from the list.  *To delete a custom category that you used in a URL filtering profile, you must set the action to None before you can delete the custom category. See Category actions in* Objects > Security Profiles > URL Filtering.

Objects > Security Profiles

Security profiles provide threat protection in Security Policy. Each Security policy rule can include one or more Security Profiles. The following are available profile types:

- Antivirus profiles to protect against worms, viruses, and trojans and to block spyware downloads. See Objects > Security Profiles > Antivirus.
- Anti-Spyware profiles to block attempts from spyware on compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers. See Objects > Security Profiles > Anti-Spyware Profile.
- Vulnerability protection profiles to stop attempts to exploit system flaws or gain unauthorized access to systems. See Objects > Security Profiles > Vulnerability Protection.
- URL filtering profiles to restrict users access to specific websites and/or website categories, such as shopping or gambling. See Objects > Security Profiles > URL Filtering.
- File blocking profiles to block selected file types, and in the specified session flow direction (inbound/outbound/both). See Objects > Security Profiles > File Blocking.
- WildFire™ analysis profiles to specify for file analysis to be performed locally on the WildFire appliance or in the WildFire cloud. See Objects > Security Profiles > WildFire Analysis.
- Data filtering profiles that help prevent sensitive information such as credit card or social security numbers from leaving a protected network. See Objects > Security Profiles > Data Filtering.
- DoS Protection profiles are used with DoS Protection policy rules to protect the firewall from high-volume single-session and multiple-session attacks. See Objects > Security Profiles > DoS Protection.
- Mobile Network Protection profiles enable the firewall to inspect, validate and filter GTP traffic.

In additional to individual profiles, you can combine profiles that are often applied together, and create Security Profile groups (**Objects** > **Security Profile Groups**).

Actions in Security Profiles

The action specifies how the firewall responds to a threat event. Every threat or virus signature that is defined by Palo Alto Networks includes a default action, which is typically either set to **Alert,** which informs you using the option you have enabled for notification, or to **Reset Both**, which resets both sides of the connection. However, you can define or override the action on the firewall. The following actions are applicable when defining Antivirus profiles, Anti-Spyware profiles, Vulnerability Protection profiles, custom spyware objects, custom vulnerability objects, or DoS Protection profiles.

Action	Description	Antivirus Profile	Anti-Spyware profile	Vulnerability Protection Profile	Custom Object—Spyware and Vulnerability	DoS Protection Profile
Default	Takes the default action that is specified internally for each threat signature. For antivirus profiles, it takes the default action for the virus signature.	✓	✓	✓	—	Random Early Drop

Action	Description	Antivirus Profile	Anti-Spyware profile	Vulnerability Protection Profile	Custom Object—Spyware and Vulnerability	DoS Protection Profile
Allow	Permits the application traffic.  *The Allow action does not generate logs related to the signatures or profiles.*	✓	✓	✓	✓	—
Alert	Generates an alert for each application traffic flow. The alert is saved in the threat log.	✓	✓	✓	✓	✓ Generates an alert when attack volume (cps) reaches the Alarm threshold set in the profile.
Drop	Drops the application traffic.	✓	✓	✓	✓	—
Reset Client	For TCP, resets the client-side connection. For UDP, the connection is dropped	✓	✓	✓	✓	—
Reset Server	For TCP, resets the server-side connection. For UDP, the connection is dropped	✓	✓	✓	✓	—

Action	Description	Antivirus Profile	Anti-Spyware profile	Vulnerability Protection Profile	Custom Object—Spyware and Vulnerability	DoS Protection Profile
Reset Both	For TCP, resets the connection on both client and server ends. For UDP, the connection is dropped	✓	✓	✓	✓	–
Block IP	Blocks traffic from either a source or a source-destination pair; Configurable for a specified period of time.	–	✓	✓	✓	✓
Sinkhole	This action directs DNS queries for malicious domains to a sinkhole IP address. The action is available for Palo Alto Networks DNS-signatures and for custom domains included in Objects > External Dynamic Lists.	–	–	–	–	–
Random Early Drop	Causes the firewall to randomly drop packets when connections per second reach the Activate Rate threshold in a DoS Protection profile applied to a DoS Protection rule.	–	–	–	–	✓
SYN Cookies	Causes the firewall to generate SYN cookies to authenticate a SYN from a client when connections per second reach the Activate Rate Threshold in a DoS Protection profile	–	–	–	–	✓

Action	Description	Antivirus Profile	Anti-Spyware profile	Vulnerability Protection Profile	Custom Object—Spyware and Vulnerability	DoS Protection Profile
	applied to a DoS Protection rule.					

You cannot delete a profile that is used in a policy rule; you must first remove the profile from the policy rule.

Objects > Security Profiles > Antivirus

Use the **Antivirus Profiles** page to configure options to have the firewall scan for viruses on the defined traffic. Set the applications that should be inspected for viruses and the action to take when a virus is detected. The default profile inspects all of the listed protocol decoders for viruses, generates alerts for Simple Mail Transport Protocol (SMTP), Internet Message Access Protocol (IMAP), and Post Office Protocol Version 3 (POP3), and takes the default action for other applications (alert or deny), depending on the type of virus detected. The profile will then be attached to a Security policy rule to determine the traffic traversing specific zones that will be inspected.

Customized profiles can be used to minimize antivirus inspection for traffic between trusted security zones, and to maximize the inspection of traffic received from untrusted zones, such as the Internet, as well as the traffic sent to highly sensitive destinations, such as server farms.

To add a new Antivirus profile, select Add and enter the following settings:

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of antivirus profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared (Panorama only)	Select this option if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this Antivirus profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.
Action Tab Specify the action for the different types of traffic, such as FTP and HTTP.	
Enable Packet Capture	Select this option if you want to capture identified packets.
Decoders and Actions	For each type of traffic that you want to inspect for viruses, select an action from the drop-down. You can define different actions for standard antivirus signatures (**Signature Action** column), signatures generated by the WildFire system (**WildFire Signature Action** column), and malicious threats detected in real-time by the WildFire Inline ML models (**WildFire Inline ML Action** column). Some environments may have requirements for a longer soak time for antivirus signatures, so this option enables the ability to set different actions for the two antivirus signature types provided by Palo Alto Networks. For

Field	Description
	example, the standard antivirus signatures go through a longer soak period before being released (24 hours), versus WildFire signatures, which can be generated and released within 15 minutes after a threat is detected. Because of this, you may want to choose the alert action on WildFire signatures instead of blocking. *For the best security, clone the default Antivirus profile and set the Action and WildFire Action for all the decoders to reset-both and attach the profile to all Security policy rules that allow traffic.*
Application Exceptions and Actions	The **Applications Exceptions** table allows you to define applications that will not be inspected. For example, to block all HTTP traffic except for a specific application, you can define an antivirus profile for which the application is an exception. **Block** is the action for the HTTP decoder, and **Allow** is the exception for the application. For each application exception, select the action to be taken when the threat is detected. For a list of actions, see Actions in Security Profiles. To find an application, start typing the application name in the text box. A matching list of applications is displayed, and you can make a selection. *If you believe a legitimate application is incorrectly identified as carrying a virus (false positive), open a support case with TAC so Palo Alto Networks can analyze and fix the incorrectly identified virus. When the issue is resolved, remove the exception from the profile.*

Signature Exceptions Tab

Use the **Signature Exception** tab to define a list of threats that will be ignored by the antivirus profile.

Only create an exception if you are sure an identified virus is not a threat (false positive). If you believe you have discovered a false positive, open a support case with TAC so Palo Alto Networks can analyze and fix the incorrectly identified virus signature. When the issue is resolved, remove the exception from the profile immediately.

Threat ID	To add specific threats that you want to ignore, enter one Threat ID at a time and click **Add**. Threat IDs are presented as part of the threat log information. Refer to Monitor > Logs.

WildFire Inline ML Tab

Use the **WildFire Inline ML** tab to enable and configure real-time WildFire analysis of files using a firewall-based machine learning model.

Palo Alto Networks recommends forwarding samples to the WildFire cloud when Wildfire inline ML is enabled. This allows samples that trigger a false-positive to be automatically corrected upon secondary analysis. Additionally, it provides data for improving ML models for future updates.

Field	Description
Available Models	For each available WildFire inline ML **Model**, you can select one of the following action settings: • **enable (inherit per-protocol actions)**—Traffic is inspected according to your selections in the **WildFire Inline ML Action** column in the decoders section of the **Action** tab. • **alert-only (override more strict actions to alert)**—Traffic is inspected according to your selections in the **WildFire Inline ML Action** column in the decoders section of the **Action** tab. Any action with a severity level higher than alert (drop, reset-client, reset-server, reset-both) will be overridden to alert, allowing traffic to pass while generating and saving an alert in the threat logs. • **disable (for all protocols)**—Traffic is allowed to pass without any policy action.
File Exceptions	The **File Exceptions** table allows you to define specific files that you do not want analyzed, such as false-positives. To create a new file exception entry, **Add** a new entry and provide the partial hash, filename, and description of the file that you want to exclude from enforcement. To find an existing file exception, start typing the partial hash value, file name, or description in the text box. A list of file exceptions matching any of those values are displayed. *You can find partial hashes in the threat logs (Monitor > Logs > Threat).*

Objects > Security Profiles > Anti-Spyware Profile

You can attach an Anti-Spyware profile to a Security policy rule to detect connections initiated by spyware and various types of command-and-control (C2) malware installed on systems on your network. You can choose between two predefined Anti-Spyware profiles to attach to a Security policy rule. Each profile has a set of predefined rules (with threat signatures) organized by the severity of the threat; each threat signature includes a *default* action that is specified by Palo Alto Networks.

- Default—The default profile uses the default action for every signature, as specified by the Palo Alto Networks content package when the signature is created.
- Strict—The strict profile overrides the action defined in the signature file for critical, high, and medium severity threats, and sets it to the **reset-both** action. The default action is taken with low and informational severity threats.
- You can also create custom profiles. You can, for example, reduce the stringency for Anti-Spyware inspection for traffic between trusted security zones, and maximize the inspection of traffic received from the internet, or traffic sent to protected assets such as server farms.

The following tables describe the Anti-Spyware profile settings:

Anti-Spyware Profile Settings	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of Anti-Spyware profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared (Panorama only)	Select this option if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this Anti-Spyware profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.
Signature Policies Tab Anti-Spyware rules allow you to define a custom severity and action to take on any threat, a specific threat name that contains the text that you enter, and/or by a threat category, such as adware. **Add** a new rule, or you can select an existing rule to and select **Find Matching Signatures** to filter threat signatures based on that rule.	
Rule Name	Specify the rule name.

Anti-Spyware Profile Settings	Description
Threat Name	Enter **any** to match all signatures, or enter text to match any signature containing the entered text as part of the signature name.
Category	Choose a category, or choose **any** to match all categories.
Action	Choose an action for each threat. For a list of actions, see Actions in Security Profiles. The **Default** action is based on the pre-defined action that is part of each signature provided by Palo Alto Networks. To view the default action for a signature, select **Objects** > **Security Profiles** > **Anti-Spyware** and **Add** or select an existing profile. Click the **Exceptions** tab and then click **Show all signatures** to see a list of all signatures and the associated **Action**.  *For the best security, use the Action settings in the predefined strict profile.*
Packet Capture	Select this option if you want to capture identified packets. Select **single-packet** to capture one packet when a threat is detected, or select the **extended-capture** option to capture from 1 to 50 packets (default is 5 packets). Extended-capture provides more context about the threat when analyzing the threat logs. To view the packet capture, select **Monitor** > **Logs** > **Threat**, locate the log entry you are interested in, and then click the green down arrow in the second column. To define the number of packets to capture, select **Device** > **Setup** > **Content-ID** and then edit the Content-ID™ Settings. If the action for a given threat is allow, the firewall does not trigger a Threat log and does not capture packets. If the action is alert, you can set the packet capture to single-packet or extended-capture. All blocking actions (drop, block, and reset actions) capture a single packet. The content package on the device determines the default action.  *Enable extended-capture for critical, high, and medium severity events. Use the default extended-capture value of 5 packets, which provides enough information to analyze the threat in most cases. (Too much packet capture traffic may result in dropping packet captures.) Don't enable extended-capture for informational and low severity events because it's not very useful compared to capturing information about higher severity events and creates a relatively high volume of low-value traffic.*
Severity	Choose a severity level (**critical**, **high**, **medium**, **low**, or **informational**).

Signature Exceptions Tab

Allows you to change the action for a specific signature. For example, you can generate alerts for a specific set of signatures and block all packets that match all other signatures. Threat exceptions are usually configured when false-positives occur. To make management of threat exceptions easier, you can add threat exceptions directly from the **Monitor** > **Logs** > **Threat** list. Ensure that you obtain the latest

Anti-Spyware Profile Settings	Description
content updates so that you are protected against new threats and have new signatures for any false-positives.	
Exceptions	**Enable** each threat for which you want to assign an action or select **All** to respond to all listed threats. The list depends on the selected host, category, and severity. If the list is empty, there are no threats for the current selections. Use IP Address Exemptions to add IP address filters to a threat exception. If IP addresses are added to a threat exception, the threat exception action for that signature overrides the action for a rule only when the signature is triggered by a session with a source or destination IP address that matches an IP address in the exception. You can add up to 100 IP addresses per signature. With this option, you do not have to create a new policy rule and new vulnerability profile to create an exception for a specific IP address. *Create an exception only if you are sure that a signature identified as spyware is not a threat (it is a false positive). If you believe you discovered a false positive, open a support case with TAC so Palo Alto Networks can analyze and fix the incorrectly identified signature. As soon as the issue is resolved, remove the exception from the profile.*
DNS Policies Tab The **DNS Policies** settings provide an additional method of identifying infected hosts on a network. These signatures detect specific DNS lookups for host names that have been associated with DNS-based threats.	
You can configure specific DNS signature sources with separate policy actions, log severity level, and packet capture settings. Hosts that perform DNS queries for malware domains will appear in the botnet report. Additionally, you can specify sinkhole IPs in the **DNS Sinkhole Settings** if you are sinkholing malware DNS queries.	
DNS Signature Source	Allows you to select the lists for which you want to enforce an action when a DNS query occurs. There are two default DNS signature policy options: • **Palo Alto Networks Content**—A local downloadable signature list that is updated through dynamic content updates. • **DNS Security**—A cloud-based DNS security service that performs pro-active analysis of DNS data and provides real-time access to the complete Palo Alto Networks DNS signature database. *This service requires the purchase and activation of the DNS Security license in addition to a Threat Prevention license.* • **External Dynamic Lists**—Dynamic domain lists that have been created can be used to enforce specific actions based on the list type, for example, as an allow list. By default, policy actions for domain lists are configured to **Allow** and take precedence over all other signature types.

Anti-Spyware Profile Settings	Description
	This service requires the purchase and activation of the DNS Security license in addition to a Threat Prevention license. By default, the locally-accessed Palo Alto Networks Content DNS signatures are sinkholed, while the cloud-based DNS Security is set to allow. If you want to enable sinkholing using DNS Security, you must configure the action on DNS queries to sinkhole. The default address used for sinkholing belongs to Palo Alto Networks (sinkhole.paloaltonetworks.com). This address is not static and can be modified through content updates on the firewall or Panorama. **Add** a new list and select the External Dynamic List of type Domain that you created. To create a new list, see Objects > External Dynamic Lists.
Log Severity	Allows you to specify the log severity level that is recorded when the firewall detects a domain matching a DNS signature.
Policy Action	Choose an action to take when DNS lookups are made to known malware sites. The options are **alert**, **allow**, **block**, or **sinkhole**. The default action for Palo Alto Networks DNS signatures is **sinkhole**. The DNS sinkhole action provides administrators with a method of identifying infected hosts on the network using DNS traffic, even when the firewall is north of a local DNS server (for example, the firewall cannot see the originator of the DNS query). When a threat prevention license is installed and an Anti-Spyware profile is enabled in a Security Profile, the DNS-based signatures trigger on DNS queries directed at malware domains. In a typical deployment where the firewall is north of the local DNS server, the threat log identifies the local DNS resolver as the source of the traffic rather than the actual infected host. Sinkholing malware DNS queries solves this visibility problem by forging responses to the queries directed at malicious domains, so that clients attempting to connect to malicious domains (for command-and-control, for example) instead attempt connections to an IP address specified by the administrator. Infected hosts can then be easily identified in the traffic logs because any host that attempts to connect to the sinkhole IP are most likely infected with malware. *Enable DNS sinkhole when the firewall can't see the originator of the DNS query (typically when the firewall is north of the local DNS server) so you can identify infected hosts. If you can't sinkhole the traffic, block it.*
Packet Capture	Select this option for a given source if you want to capture identified packets. *Enable packet capture on sinkholed traffic so you can analyze it and get information about the infected host.*

Anti-Spyware Profile Settings	Description
DNS Sinkhole Settings	After sinkhole action is defined for a DNS signature source, specify an IPv4 and/or IPv6 address that will be used for sinkholing. By default, the sinkhole IP address is set to a Palo Alto Networks server. You can then use the traffic logs or build a custom report that filters on the sinkhole IP address and identify infected clients. The following is the sequence of events that will occur when an DNS request is sinkholed: Malicious software on an infected client computer sends a DNS query to resolve a malicious host on the Internet. The client's DNS query is sent to an internal DNS server, which then queries a public DNS server on the other side of the firewall. The DNS query matches a DNS entry in the specified DNS signature database source, so the sinkhole action will be performed on the query. The infected client then attempts to start a session with the host, but uses the forged IP address instead. The forged IP address is the address defined in the Anti-Spyware profile DNS Signatures tab when the sinkhole action is selected. The administrator is alerted of a malicious DNS query in the threat log, and can then search the traffic logs for the sinkhole IP address and can easily locate the client IP address that is trying to start a session with the sinkhole IP address.
DNS Exceptions Tab The DNS signature exceptions allow you to exclude specific threat IDs from policy enforcement as well as specify domain/FQDN allow lists for approved domain sources. To add specific threats that you want to exclude from policy, select or search for a **Threat ID** and click **Enable**. Each entry provides the threat **Threat ID**, **Name**, and **FQDN** of the object. To **Add** a domain or FQDN allow list, provide the location of the allow list as well as an appropriate description.	

Objects > Security Profiles > Vulnerability Protection

A Security policy rule can include specification of a Vulnerability Protection profile that determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. There are two predefined profiles available for the Vulnerability Protection feature:

- The **default** profile applies the default action to all client and server critical, high, and medium severity vulnerabilities. It does not detect low and informational vulnerability protection events. The Palo Alto Networks content package on the device determines the default action.
- The **strict** profile applies the block response to all client and server critical, high and medium severity spyware events and uses the default action for low and informational vulnerability protection events.

Customized profiles can be used to minimize vulnerability checking for traffic between trusted security zones, and to maximize protection for traffic received from untrusted zones, such as the Internet, as well as the traffic sent to highly sensitive destinations, such as server farms. To apply Vulnerability Protection profiles to Security policies, refer to Policies > Security.

Apply a Vulnerability Protection profile to every Security Policy rule that allows traffic to protect against buffer overflows, illegal code execution, and other attempts to exploit client- and server-side vulnerabilities.

The Rules settings specify collections of signatures to enable, as well as actions to be taken when a signature within a collection is triggered.

The Exceptions settings allows you to change the response to a specific signature. For example, you can block all packets that match a signature, except for the selected one, which generates an alert. The **Exception** tab supports filtering functions.

The **Vulnerability Protection** page presents a default set of columns. Additional columns of information are available by using the column chooser. Click the arrow to the right of a column header and select the columns from the Columns sub-menu.

The following tables describe the Vulnerability Protection profile settings:

Vulnerability Protection Profile Settings	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of Vulnerability Protection profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared (Panorama only)	Select this option if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the **Device Group** selected in the **Objects** tab.

Vulnerability Protection Profile Settings	Description
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this Vulnerability Protection profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.
Rules Tab	
Rule Name	Specify a name to identify the rule.
Threat Name	Specify a text string to match. The firewall applies a collection of signatures to the rule by searching signature names for this text string.
CVE	Specify common vulnerabilities and exposures (CVEs) if you want to limit the signatures to those that also match the specified CVEs. Each CVE is in the format CVE-yyyy-xxxx, where yyyy is the year and xxxx is the unique identifier. You can perform a string match on this field. For example, to find vulnerabilities for the year 2011, enter “2011”.
Host Type	Specify whether to limit the signatures for the rule to those that are client side, server side, or either (**any**).
Severity	Select severities to match (**informational**, **low**, **medium**, **high**, or **critical**) if you want to limit the signatures to those that also match the specified severities.
Action	Choose the action to take when the rule is triggered. For a list of actions, see Actions in Security Profiles. The **Default** action is based on the pre-defined action that is part of each signature provided by Palo Alto Networks. To view the default action for a signature, select **Objects** > **Security Profiles** > **Vulnerability Protection** and **Add** or select an existing profile. Click the **Exceptions** tab and then click **Show all signatures** to see a list of all signatures and the associated **Action**.  *For the best security, set the Action for both client and server critical, high, and medium severity events to reset-both and use the default action for Informational and Low severity events.*
Packet Capture	Select this option if you want to capture identified packets. Select **single-packet** to capture one packet when a threat is detected, or select the **extended-capture** option to capture from 1 to 50 packets (default is 5 packets). Extended-capture provides more context to the threat when analyzing the threat logs. To view the packet capture, select **Monitor** > **Logs** > **Threat** and locate the log entry you are interested in and then click the green down arrow in the second column. To define the number of packets that should be captured, select **Device** > **Setup** > **Content-ID** and then edit the Content-ID Settings.

Vulnerability Protection Profile Settings	Description
	If the action for a given threat is allow, the firewall does not trigger a Threat log and does not capture packets. If the action is alert, you can set the packet capture to single-packet or extended-capture. All blocking actions (drop, block, and reset actions) capture a single packet. The content package on the device determines the default action. *Enable extended-capture for critical, high, and medium severity events and single-packet capture for low severity events. Use the default extended-capture value of 5 packets, which provides enough information to analyze the threat in most cases. (Too much packet capture traffic may result in dropping packet captures.) Don't enable packet capture for informational events because it's not very useful compared to capturing information about higher severity events and creates a relatively high volume of low-value traffic.* *Apply extended packet capture using the same logic you use to decide what traffic to log—take extended captures of the traffic you log, including traffic you block.*
Exceptions Tab	
Enable	Select **Enable** for each threat for which you want to assign an action, or select **All** to respond to all listed threats. The list depends on the selected host, category, and severity. If the list is empty, there are no threats for the current selections.
ID	
Vendor ID	Specify vendor IDs if you want to limit the signatures to those that also match the specified vendor IDs. For example, the Microsoft vendor IDs are in the form MSyy-xxx, where yy is the two-digit year and xxx is the unique identifier. For example, to match Microsoft for the year 2009, enter "MS09" in the Search field.
Threat Name	*Only create a threat exception if you are sure an identified threat is not a threat (false positive). If you believe you have discovered a false positive, open a support case with TAC so Palo Alto Networks can investigate the incorrectly identified threat. When the issue is resolved, remove the exception from the profile immediately.* The vulnerability signature database contains signatures that indicate a brute force attack; for example, Threat ID 40001 triggers on an FTP brute force attack. Brute-force signatures trigger when a condition occurs in a certain time threshold. The thresholds are pre-configured for brute force signatures, and can be changed by clicking edit ( ) next to the threat name on the **Vulnerability** tab (with the **Custom** option selected). You

Vulnerability Protection Profile Settings	Description
	can specify the number of hits per unit of time and whether the threshold applies to source, destination, or source-and-destination. Thresholds can be applied on a source IP, destination IP or a combination of source IP and destination IP. The default action is shown in parentheses.
IP Address Exemptions	Click into the **IP Address Exemptions** column to **Add** IP address filters to a threat exception. When you add an IP address to a threat exception, the threat exception action for that signature will take precedence over the rule's action only if the signature is triggered by a session with either a source or destination IP address matching an IP address in the exception. You can add up to 100 IP addresses per signature. You must enter a unicast IP address (that is, an address without a netmask), such as 10.1.7.8 or 2001:db8:123:1::1. By adding IP address exemptions, you do not have to create a new policy rule and new vulnerability profile to create an exception for a specific IP address.
Rule	
CVE	The **CVE** column shows identifiers for common vulnerabilities and exposures (CVE). These unique, common identifiers are for publicly known information security vulnerabilities.
Host	
Category	Select a vulnerability category if you want to limit the signatures to those that match that category.
Severity	
Action	Choose an action from the drop-down, or choose from the **Action** drop-down at the top of the list to apply the same action to all threats.
Packet Capture	Select **Packet Capture** if you want to capture identified packets.
Show all signatures	Enable **Show all signatures** to list all signatures. If **Show all signatures** is disabled, only the signatures that are exceptions are listed.

Objects > Security Profiles > URL Filtering

You can use URL filtering profiles to not only control access to web content, but also to control how users interact with web content.

What are you looking for?	See:
Control access to websites based on URL category.	URL Filtering Categories
Detect corporate credential submissions, and then decide the URL categories to which users can submit credentials.	User Credential Detection URL Filtering Categories
Block search results if the end user is not using the strictest safe search settings.	URL Filtering Settings
Enable logging of HTTP headers.	URL Filtering Settings
Control access to websites using custom HTTP Headers.	HTTP Header Insertion
Enable inline ML to analyze web pages in real-time to determine if it contains malicious content.	URL Filtering Inline ML
Looking for more?	• Learn more about how to configure URL Filtering. • Use URL categories to Prevent Credential Phishing. • To create custom URL categories, select Objects > Custom Objects > URL Category. • To import a list of URLs that you want to enforce, select Objects > External Dynamic Lists.

URL Filtering General Settings

The following table describes the general URL filtering settings.

General Settings	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of URL filtering profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared	Select this option if you want the profile to be available to:

General Settings	Description
	• Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this URL Filtering profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.

URL Filtering Categories

Select **Objects** > **Security Profiles** > **URL Filtering** > **Categories** to control access to websites based on URL categories.

Categories Settings	Description
Category	Displays the URL categories and lists for which you can define web access and usage policy. By default, the **Site Access** and **User Credential Submission** permissions for all categories are set to **Allow**. URL categories and lists are grouped into three drop-downs: • **Custom URL Categories**—Select Objects > Custom Objects > URL Category to define a custom URL category. You can base custom URL categories on a list of URLs or on multiple predefined categories. • **External Dynamic URL Lists**— Select Objects > External Dynamic Lists to enable the firewall to import a list of URLs from a web server. • **Pre-defined Categories**—Lists all URL categories defined by PAN-DB, the Palo Alto Networks URL, and the IP cloud database.  *Block all known dangerous URL categories to protect against exploit infiltration, malware download, command-and-control activity, and data exfiltration: command-and-control, copyright-infringement, dynamic-dns, extremism, malware, phishing, proxy-avoidance-and-anonymizers, unknown, newly-registered-domain, grayware, and parked.* *To phase in a block policy, set categories to continue and create a custom response page to educate users about your use policy and alert them that they are visiting a site that potentially poses a threat. After a suitable period of time, transition to a policy that blocks these potentially malicious sites.*
Site Access	For each URL category, select the action to take when a user attempts to access a URL in that category: • **alert**—Allows access to the web site but adds an alert to the URL log each time a user accesses the URL.

Categories Settings	Description
	 *Set alert as the Action for categories of traffic that you don't block so that it logs the access attempt and provides visibility into the traffic.* • **allow**—Allows access to the web site.  *Because allow doesn't log unblocked traffic, set alert as the Action for categories of traffic you don't block if you want to log the access attempts and provide visibility into that traffic.* • **block**—Blocks access to the website. If the Site Access to a URL category is set to block, then the User Credential Submission permissions are automatically also set to block. • **continue**—Displays a warning page to users to discourage them from accessing the website. The user must then choose to **Continue** to the website if they decide to ignore the warning.  *The continue (warning) pages are not displayed properly on client machines that are configured to use a proxy server.* • **override**—Displays a response page that prompts the user to enter a valid password to gain access to the site. Configure URL Admin Override settings (**Device** > **Setup** > **Content ID**) to manage password and other override settings. (See also the Management Settings table in Device > Setup > Content-ID).  *The override pages are not displayed properly on client machines that are configured to use a proxy server.* • **none** (custom URL category only)—If you created custom URL categories, set the action to **none** to allow the firewall to inherit the URL filtering category assignment from your URL database vendor. Setting the action to **none** gives you the flexibility to ignore custom categories in a URL filtering profile while allowing you to use the custom URL category as a match criteria in policy rules (Security, Decryption, and QoS) to make exceptions or to enforce different actions. To delete a custom URL category, you must set the action to **none** in any profile where the custom category is used. For information on custom URL categories, see Objects > Custom Objects > URL Category.
User Credential Submission	For each URL category, select **User Credential Submissions** to allow or disallow users from submitting valid corporate credentials to a URL in that category. Before you can control user credential submissions based on URL category, you must enable credential submission detection (select the **User Credential Detection** tab). URL categories with the **Site Access** set to block are set to automatically also block user credential submissions. • **alert**—Allows users to submit credentials to the website, but generate a URL Filtering log each time a user submits credentials to sites in this category. • **allow** (default)—Allows users to submit credentials to the website.

Categories Settings	Description
	• **block**—Blocks users from submitting credentials to the website. A default anti-phishing response page blocks user credential submissions. • **continue**—Displays a response page to users that prompts them to select **Continue** to submit credentials to the site. By default, an anti-phishing continue page displays to warn users when they attempt to submit credentials to sites to which credential submissions are discouraged. You can choose to create a custom response page to warn users against phishing attempts or to educate them against reusing valid corporate credentials on other websites.
Check URL Category	Click to access the PAN-DB URL Filtering database, where you can enter a URL or IP address to view categorization information.
Dynamic URL Filtering (disabled by default) (Configurable for BrightCloud only)	Select to enable cloud lookup for categorizing the URL. This option is invoked if the local database is unable to categorize the URL. If the URL is unresolved after a 5 second timeout, the response is displayed as `Not resolved URL`. *With PAN-DB, this option is enabled by default and is not configurable.*

URL Filtering Settings

Select **Objects** > **Security Profiles** > **URL Filtering** > **URL Filtering Settings** to enforce safe search settings, and to enable logging of HTTP headers.

URL Filtering Settings	Descriptions
Log container page only Default: Enabled	Select this option to log only the URLs that match the content type that is specified. The firewall doesn't log related web links during the session, such as advertisements and content links, which reduces the logging and memory load while still logging relevant URLs. *If you use proxies that mask the original IP address of the source, enable the HTTP Header Logging X-Forwarded-For option to preserve the original IP address of the user who initiate the web page request.*
Enable Safe Search Enforcement Default: Disabled A URL filtering license is not required to use this feature.	Select this option to enforce strict safe search filtering. Many search engines have a safe search setting that filters out adult images and videos in search query return traffic. When you select the setting to Enable Safe Search Enforcement, the firewall blocks search results if the end user is not using the strictest safe search settings in the search query. The firewall can enforce safe search for the following search providers: Google, Yahoo, Bing, Yandex, and YouTube. This is a best-effort setting and is not guaranteed by the search providers to work with every website. To use safe search enforcement you must enable this setting and then attach the URL filtering profile Security policy rule. The firewall will then block any

URL Filtering Settings	Descriptions
	matching search query return traffic that is not using the strictest safe search settings. *If you are performing a search on Yahoo Japan (yahoo.co.jp) while logged into your Yahoo account, the lock option for the search setting must also be enabled.* *To prevent users from bypassing this feature by using other search providers, configure the URL filtering profile to block the search-engines category and then allow access to Bing, Google, Yahoo, Yandex, and YouTube.*
HTTP Header Logging	Enabling HTTP Header Logging provides visibility into the attributes included in the HTTP request sent to a server. When enabled one or more of the following attribute-value pairs are recorded in the URL Filtering log: • User-Agent—The web browser that the user used to access the URL. This information is sent in the HTTP request to the server. For example, the User-Agent can be Internet Explorer or Firefox. The User-Agent value in the log supports up to 1024 characters. • Referer—The URL of the web page that linked the user to another web page; it is the source that redirected (referred) the user to the web page that is being requested. The referer value in the log supports up to 256 characters. • X-Forwarded-For—The header field option that preserves the IP address of the user who requested the web page. It allows you to identify the IP address of the user, which is particularly useful if you have a proxy server on your network or you have implemented Source NAT, that is masking the user's IP address such that all requests seem to originate from the proxy server's IP address or a common IP address. The x-forwarded-for value in the log supports up to 128 characters.

User Credential Detection

Select **Objects** > **Security Profiles** > **URL Filtering** > **User Credential Detection** to enable the firewall to detect when users submit corporate credentials.

Configure user credential detection so that users can submit credentials only to sites in specified URL categories, which reduces the attack surface by preventing credential submission to sites in untrusted categories. If you block all the URL categories in a URL Filtering profile for user credential submission, you don't need to check credentials.

The firewall uses one of three methods to detect valid credentials submitted to web pages. Each method requires User-ID™, which enables the firewall to compare username and password submissions to web pages against valid, corporate credentials. Select one of these methods to then continue to Prevent Credential Phishing based on URL category.

You must configure the firewall to decrypt traffic that you want to monitor for user credentials.

User Credential Detection Settings	Description
IP User	This credential detection method checks for valid username submissions. You can use this method to detect credential submissions that include a valid corporate username (regardless of the accompanying password). The firewall determines a username match by verifying that the username matches the user logged in the source IP address of the session. To use this method, the firewall matches the submitted username against its IP-address-to-username mapping table. To use this method you can use any of the user mapping methods described in Map IP Addresses to Users.
Group Mapping	The firewall determines if the username a user submits to a restricted site matches any valid corporate username. To do this, the firewall matches the submitted username to the list of usernames in its user-to-group mapping table to detect when users submit a corporate usernames to a site in a restricted category. This method only checks for corporate username submissions based on LDAP group membership, which makes it simple to configure, but more prone to false positives. You must enable group mapping to use this method.
Domain Credential	This credential detection method enables the firewall to check for a valid corporate username and the associated password. The firewall determines if the username and password a user submits matches the same user's corporate username and password. To do this, the firewall must able to match credential submissions to valid corporate usernames and passwords and verify that the username submitted maps to the IP address of the logged in user. This mode is supported only with the Windows-based User-ID agent, and requires that the User-ID agent is installed on a read-only domain controller (RODC) and equipped with the User-ID Credential Service Add-on. To use this method, you must also enable User-ID to Map IP Addresses to Users using any of the supported user mapping methods, including Authentication Policy, Authentication Portal, and GlobalProtect.™ See Prevent Credential Phishing for details on each of the methods the firewall can use to check for valid corporate credential submissions, and for steps to enable phishing prevention.
Valid Username Detected Log Severity	Set the severity for logs that indicate the firewall detected a valid username submission to a website. This log severity is associated with events where a valid username is submitted to websites with credential submission permissions to alert, block or continue. Logs that record when a user submits a valid username to a website for which credential submissions are allowed have a severity of informational. Select **Categories** to review or adjust the URL categories to which credential submissions are allowed and blocked. *Set the log severity to medium or stronger.*

HTTP Header Insertion

To enable the firewall to manage web application access by inserting HTTP headers and their values into HTTP requests, select **Objects** > **Security Profiles** > **URL Filtering** > **HTTP Header Insertion**.

The firewall supports header insertion for HTTP/1.x traffic only; the firewall does not support header insertion for HTTP/2 traffic.

You can create insertion entries based on a predefined HTTP header insertion type or you can create your own custom type. Header insertion is typically performed for custom HTTP headers but you can also insert standard HTTP headers.

Header insertion occurs when:

1. An HTTP request matches a Security policy rule with one or more configured HTTP header insertion entries.
2. A specified domain matches the domain found in the HTTP Host header.
3. The action is anything other than `block`.

The firewall can perform HTTP header insertion only for the GET, POST, PUT, and HEAD methods.

If you enable HTTP header insertion and the identified header is missing from a request, the firewall inserts the header. If the identified header already exists in the request, then the firewall overwrites the header values with the values that you specify.

Add an insertion entry or select an existing insertion entry to modify it. When needed, you can also select an insertion entry and **Delete** it.

The default block list action for a new HTTP header insertion entry is `block`. If you want a different action, go to URL Filtering Categories *and select the appropriate action. Alternatively, add the insertion entry to a profile that is configured with the desired action.*

HTTP Header Insertion Settings	Description
Name	The **Name** for this HTTP header insertion entry.
Type	The **Type** of entry you want to create. Entries can be either predefined or custom. The firewall uses content updates to populate and maintain predefined entries. To include the username in the HTTP header, select **Dynamic Fields**.
Domains	Header insertion occurs when a domain in this list matches the Host header of the HTTP request. If you are creating a predefined entry, the domain list is predefined in a content update. This is sufficient for most use cases but you can add or delete domains as needed. To create a custom entry, **Add** at least one domain to this list. Each domain name can be up to 256 characters and you can identify a maximum of 50 domains for each entry. You can use an asterisk (*) as a

HTTP Header Insertion Settings	Description
	wildcard character, which matches any request to the specified domain (for example, *.etrade.com).
Header	When you create a predefined entry, the Header list is pre-populated by a content update. This is sufficient for most use cases but you can add or delete headers as needed. When you create a custom entry, add one or more headers (up to a total of five) to this list. Header names can have up to 100 characters but cannot include spaces. To include the username in the HTTP header, select **X-Authenticated-User** then select the **Value**, or **Add** a new header.
Value	Configure the **Value** using a maximum of 512 characters. The header value varies depending on what information you want to include in the HTTP header for the specified domains. For example, manage user access to SaaS applications by selecting predefined types or by using custom entries. To include the username in the HTTP header, select the domain and username format that the security device requires: • **`($domain)\($user)`** • **`WinNT://($domain)/($user)`** Alternatively, enter a custom format using the **`($user)`** and **`($domain)`** dynamic tokens (for example, **`($user)@($domain)`**). The firewall populates the user and domain dynamic tokens using the primary username in the group mapping profile. *Use each **`($user)`** and **`($domain)`** dynamic token only once per value.*
Log	Select **Log** to enable logging of this header insertion entry.

URL Filtering Inline ML

Select **Objects** > **Security Profiles** > **URL Filtering** > **Inline ML** to enable and configure real-time analysis of web pages using a firewall-based machine learning model.

Field	Description
Use the **Inline ML** tab to enable and configure policy actions.	
Available Models	For each available inline ML model, you can select one of the following actions: • **Alert**—The website is allowed and a log entry is generated in the URL filtering log. • **Allow**—The website is allowed and no log entry is generated.

Field	Description
	• **Block**—The website is blocked and the user will not be able to continue to the website. A log entry is generated in the URL filtering log.
Exceptions	You can define URL **Exceptions** for specific web sites that you do not want analyzed, such as those that might trigger false-positives. To add URL exceptions, you must first define a valid EDL (external dynamic list) or custom URL category. Click **Add** to view and select from the available options.

Objects > Security Profiles > File Blocking

You can attach a File Blocking profile to a Security policy rule (Policies > Security) to block users from uploading or downloading specified file types or to generate an alert when a user attempts to upload or download specified file types.

For the best security, apply the predefined strict profile. If you need to support critical applications that use a file type which the strict profile blocks, clone the strict profile and make only the file type exceptions you need. Apply the cloned profile to a Security Policy rule that restricts the exception to only the sources, destinations, and users that need to use the file type. You can also use Direction to restrict the exception to uploading or downloading.

If you don't block all Windows PE files, send all unknown files to WildFire for analysis. For user accounts, set the Action to continue to help prevent drive-by downloads where malicious web sites, emails, or pop-ups cause users to inadvertently download malicious files. Educate users that a Continue prompt for a file transfer they didn't knowingly initiate may mean they are subject to a malicious download.

The following tables describe the file blocking profile settings.

File Blocking Profile Settings	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of file blocking profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared (Panorama only)	Select this option if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this File Blocking profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.
Rules	Define one or more rules to specify the action taken (if any) for the selected file types. To add a rule, specify the following and click **Add**: • **Name**—Enter a rule name (up to 31 characters). • **Applications**—Select the applications the rule applies to or select **any**. • **File Types**—Click in the file types field and then click **Add** to view a list of supported file types. Click a file type to add it to the profile and continue to add additional file types as needed. If you select **Any**, the defined action is taken on all supported file types.

File Blocking Profile Settings	Description
	• **Direction**—Select the direction of the file transfer (**Upload**, **Download**, or **Both**). • **Action**—Select the action taken when the selected file types are detected: • **alert**—An entry is added to the threat log. • **continue**—A message to the user indicates that a download has been requested and asks the user to confirm whether to continue. The purpose is to warn the user of a possible unknown download (also known as a drive-by-download) and to give the user the option of continuing or stopping the download. When you create a file blocking profile with the action **continue**, you can only choose the application **web-browsing**. If you choose any other application, traffic that matches the Security policy rule will not flow through the firewall due to the fact that the users will not be prompted with a continue page. • **block**—The file is blocked.

Objects > Security Profiles > WildFire Analysis

Use a WildFire Analysis profile to specify for WildFire file analysis to be performed locally on the WildFire appliance or in the WildFire cloud. You can specify traffic to be forwarded to the public cloud or private cloud based on file type, application, or the transmission direction of the file (upload or download). After creating a WildFire analysis profile, adding the profile to a policy (**Policies** > **Security**) further allows you apply the profile settings to any traffic matched to that policy (for example, a URL category defined in the policy).

Use the predefined default profile to forward all unknown files to WildFire for analysis. In addition, set up WildFire appliance content updates to download and install every minute so you always have the most recent support.

WildFire Analysis Profile Settings	
Name	Enter a descriptive name for the WildFire analysis profile (up to 31 characters). This name appears in the list of WildFire Analysis profiles that you can choose from when defining a Security policy rule. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Optionally describe the profile rules or the intended use for the profile (up to 255 characters).
Shared (Panorama only)	Select this option if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this Vulnerability Protection profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.
Rules	Define one or more rules to specify traffic to forward to either the WildFire public cloud or the WildFire appliance (private cloud) for analysis. • Enter a descriptive **Name** for any rules you add to the profile (up to 31 characters). • Add an **Application** so that any application traffic will be matched to the rule and forwarded to the specified analysis destination. • Select a **File Type** to be analyzed at the defined analysis destination for the rule.  *A WildFire private cloud (hosted by a WildFire appliance) does not support analysis of APK, Mac OS X, archive, and linux files.*

WildFire Analysis Profile Settings	
	• Apply the rule to traffic depending on the transmission **Direction**. You can apply the rule to upload traffic, download traffic, or both. • Select the destination for traffic to be forwarded for **Analysis**: • Select public-cloud so that all traffic matched to the rule is forwarded to the WildFire public cloud for analysis. • Select private-cloud so that all traffic matched to the rule is forwarded to the WildFire appliance for analysis.

Objects > Security Profiles > Data Filtering

Data filtering enables the firewall to detect sensitive information—such as credit card or social security numbers or internal corporate documents—and prevent this data from leaving a secure network. Before you enable data filtering, select Objects > Custom Objects > Data Patterns to define the type of data you want to filter (such as social security numbers or document titles that contain the word "confidential"). You can add several data pattern objects to a single Data Filtering profile and, when attached to a Security policy rule, the firewall scans allowed traffic for each data pattern and blocks matching traffic based on the data filtering profile settings.

Data Filtering Profile Settings	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of log forwarding profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared (Panorama only)	Select this option if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this Data Filtering profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.
Data Capture	Select this option to automatically collect the data that is blocked by the filter. *Specify a password for Manage Data Protection on the Settings page to view your captured data. Refer to* Device > Setup > Management*.*
Data Pattern	Add an existing data pattern to use for filtering or select **New** to configure a new data pattern object (Objects > Custom Objects > Data Patterns).
Applications	Specify the applications to include in the filtering rule: • Choose **any** to apply the filter to all of the listed applications. This selection does not block all possible applications, just the listed ones. • Click **Add** to specify individual applications.
File Types	Specify the file types to include in the filtering rule:

Data Filtering Profile Settings	Description
	• Choose **any** to apply the filter to all of the listed file types. This selection does not block all possible file types, just the listed ones. • Click **Add** to specify individual file types.
Direction	Specify whether to apply the filter in the upload direction, download direction, or both.
Alert Threshold	Specify the number of times the data pattern must be detected in a file to trigger an alert.
Block Threshold	Block files that contain at least this many instances of the data pattern.
Log Severity	Define the log severity recorded for events that match this data filtering profile rule.

Objects > Security Profiles > DoS Protection

DoS Protection profiles are designed for high-precision targeting and they augment Zone Protection profiles. A DoS Protection profile specifies the threshold rates at which new connections per second (CPS) trigger an alarm and an action (specified in the DoS Protection policy). The DoS Protection profile also specifies the maximum CPS rate and how long a blocked IP address remains on the Block IP list. You specify a DoS protection profile in a DoS protection policy rule, where you specify the criteria for packets to match the rule, and the policy rule determines the devices to which the profile applies.

Create DoS Protection profiles and policies to protect critical individual devices or small groups of devices, especially internet-facing devices such as web servers and database servers.

You can configure Aggregate and Classified DoS Protection profiles. You can apply an Aggregate profile, a Classified profile, or one of each type to a DoS Protection policy rule. If you apply both profile types to a rule, the firewall applies the Aggregate profile first and then applies the Classified profile if needed.

- A Classified DoS Protection profile has **Classified** selected as the **Type**. When you apply a Classified DoS Protection profile to a DoS Protection rule whose action is **Protect**, the firewall counts connections toward the profile's CPS thresholds if the packet meets the specified Address type: source-ip-only, destination-ip-only, or src-dest-ip-both.
- An Aggregate DoS Protection profile has **Aggregate** selected as the **Type**. When you apply an Aggregate DoS Protection profile a DoS Protection rule whose action is **Protect**, the firewall counts all connections (the combined number of connections for the group of devices specified in the rule) that meet the criteria for the rule toward the profile's CPS thresholds.

To apply a DoS Protection profile to a DoS Protection policy, see Policies > DoS Protection.

If you have a multiple virtual system (multi-vsys) environment and have configured the following:

- *External zones to enable inter-virtual system communication and*
- *Shared gateways to allow virtual systems to share a common interface and a single IP address for external communications, then*

The following Zone and DoS protection mechanisms are disabled on the external zone:

- *SYN cookies*
- *IP fragmentation*
- *ICMPv6*

To enable IP fragmentation and ICMPv6 protection, create a separate zone protection profile for the shared gateway.

To protect against SYN floods on a shared gateway, you can apply a SYN Flood protection profile with either Random Early Drop or SYN cookies. On an external zone, only Random Early Drop is available for SYN Flood protection.

DoS Protection Profile Settings	
Name	Enter a profile name (up to 31 characters). This name appears in the list of log forwarding profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

DoS Protection Profile Settings	
Description	Enter a description of the profile (up to 255 characters).
Shared (Panorama only)	Select this option if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this DoS Protection profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.
Type	Select one of the following profile types: • **Aggregate**—Apply the DoS thresholds configured in the profile to all connections that match the rule criteria on which this profile is applied. For example, an aggregate rule with a SYN flood **Alarm Rate** threshold of 10,000 CPS counts the combined connections of all the devices that match the DoS rule. When the total CPS for the group exceeds 10,000 CPS that triggers the alarm, regardless of how the CPS are spread across the devices. • **Classified**—Apply the DoS thresholds configured in the profile to each individual connection that matches the classification criteria (source IP address, destination IP address, or source-and-destination IP address pair). For example, a classified rule with a SYN flood **Alarm Rate** threshold of 10,000 CPS allows up to 10,000 CPS per device and triggers an alarm when any individual device specified in the DoS rule exceeds 10,000 CPS.
Flood Protection Tab	
SYN Flood tab UDP Flood tab ICMP Flood tab ICMPv6 Flood tab Other IP Flood tab	Select this option to enable the type of flood protection indicated on the tab and specify the following settings: • **Action**—(**SYN Flood** only) Action that the firewall performs if the DoS Protection policy action is **Protect** and if incoming CPS reach the **Activate Rate**. Choose one of the following: • **Random Early Drop**—Drop packets randomly when connections per second reach the **Activate Rate** threshold. • **SYN cookies**—Use SYN cookies to generate acknowledgments so that it is not necessary to drop connections during a SYN flood attack.  *Start with SYN Cookies, which treats legitimate traffic fairly but consumes more firewall resources. Monitor CPU and memory utilization, and if SYN Cookies consumes too many resources, switch to RED. Always use RED if you don't have a dedicated DDoS prevention device at the network (internet) edge to protect against large volume DoS attacks.*

DoS Protection Profile Settings	
	• **Alarm Rate**—Specify the threshold rate (CPS) to generate a DoS alarm (range is 0 to 2,000,000 cps; default is 10,000 cps). For Classified profiles, the best practice is to set the threshold to 15-20% above the device's average CPS rate to accommodate normal fluctuations and adjust the threshold if you receive too many alarms. For Aggregate profiles, the best practice is to set the threshold to 15-20% above the group's average CPS rate. Monitor and adjust the thresholds as needed. • **Activate Rate**—Specify the threshold rate (cps) at which a DoS response is activated. The DoS response is configured in the **Action** field of the DoS Protection profile (Random Early Drop or SYN cookies). The **Activate Rate** range is 0 to 2,000,000 cps; default is 10,000 cps. If the profile **Action** is **Random Early Drop** (RED), when incoming connections per second reach the **Activate Rate** threshold, RED occurs. If the CPS rate increases, the RED rate increases according to an algorithm. The firewall continues with RED until the CPS rate reaches the **Max Rate** threshold. Classified profiles apply exact CPS limits to individual devices and you base those limits on the capacity of the protected devices, so you don't need to throttle CPS gradually and can set the **Activate Rate** to the same threshold as the **Max Rate**. Set the **Activate Rate** lower than the **Max Rate** only if you want to begin dropping traffic to an individual server before it reaches the **Max Rate**. For Aggregate profiles, set the threshold just above the peak CPS rate for the group. Monitor and adjust the thresholds as needed. • **Max Rate**—Specify the threshold rate of incoming connections per second the firewall allows. At the **Max Rate** threshold, the firewall drops 100% of new connections (range is 2 to 2,000,000 cps; default is 40,000 cps.) For Classified profiles, base the **Max Rate** on the capacity of the devices you're protecting so they can't be flooded. For Aggregate profiles, set the **Max Rate** to 80-90% of the group's capacity. Monitor and adjust the thresholds as needed. • **Block Duration**—Specify the length of time (seconds) during which the offending IP address remains on the Block IP list and connections with the IP address are blocked. The firewall doesn't count packets that arrive during the block duration toward the Alarm Rate, Activate Rate, or Max Rate thresholds (range is 1 to 21,600 seconds; default is 300 seconds).
Resources Protection Tab	
Sessions	Select this option to enable resources protection.
Maximum Concurrent Sessions	Specify the maximum number of concurrent sessions. • For the **Aggregate** profile type, this limit applies to all traffic hitting the DoS Protection rule on which the DoS Protection profile is applied. • For the **Classified** profile type, this limit applies to the traffic on a classified basis (source IP, destination IP or source-and-destination IP)

DoS Protection Profile Settings	
	hitting the DoS Protection rule to which the DoS Protection profile is applied.

Objects > Security Profiles > Mobile Network Protection

The Mobile Network Protection profile enables the firewall to inspect GTP and HTTP/2 in 5G Service Based Architecture (SBA) traffic. To view this profile, you must enable GTP Security in Device > Setup > Management.

Use the options in this profile to enable stateful inspection of 5G HTTP/2, GTP v1-C, GTP v2-C, and GTP-U, to enable protocol validation for GTPv1-C, GTP v2-C, and GTP-U, and to enable GTP-U content inspection to scan user data within GTP-U tunnels. It also enables you to filter GTP sessions based on APN, IMSI/IMSI-Prefix, and RAT, and to prevent end-user IP address spoofing.

GTP Inspection Profile Settings	
GTP Inspection	
GTP-C	• Select **Stateful Inspection** to enable the firewall to inspect **GTPv1-C** or **GTPv2-C** or both. When you enable stateful inspection, the firewall uses the source IP, source port, destination IP, destination port, protocol, and the Tunnel Endpoint IDs (TEID) to keep track of a GTP session. It also checks and validates the order of the different types of GTP messages that are used to establish a GTP tunnel. The TEID uniquely identifies the GSN tunnel endpoints. The tunnels for an uplink and a downlink are separate and use a different TEID. • Select the **Action**—**Block** or **Alert**—that the firewall takes upon a validity check failure. The alert action allows the traffic but generates a log; the block action denies the traffic and generates a log. • Specify the validity checks that the firewall must perform on a GTP header and the Information Elements (IE) in a payload. The firewall uses the block or alert action you select below for handling the error. You can configure the firewall to validate: • **Reserved IE**—Checks for the GTPv1-C or GTPv2-C messages that use reserved IE values. • **Order of IE** (GTPv1-C only)—Checks that the order of IEs in GTPv1-C messages is accurate. • **Length of IE**—Checks for the GTPv1-C or GTPv2-C messages with invalid IE length. • **Reserved field in header**—Checks for malformed packets that use invalid values or reserved values in a header. • **Unsupported message type**—Checks for unknown or incorrect message types.
GTP-U	Enabling stateful inspection for either GTPv1-C and/or GTPv2-C, automatically enables GTPU-U stateful inspection. You can specify the following validity checks for GTP-U payloads. • **Reserved IE**—Checks for the GTP-U messages that use reserved IE values in the payload.

GTP Inspection Profile Settings	
	• **Order of IE**—Checks that the order of the IEs in GTP-U messages is correct. • **Length of IE**—Checks for messages with invalid IE length. • **Reserved field in header**—Checks for malformed packets that use invalid values or reserved values in a header. • **Unsupported message type**—Checks for unknown or incorrect message types. In addition you can also configure an allow, block or alert action for: • **End User IP Address Spoofing**—Configure the firewall to block or alert when the source IP address in a GTP-U packet from the subscriber user equipment is not the same as the IP address in the corresponding GTP-C message exchanged during tunnel set up. • **GTP-in-GTP**—You can configure the firewall to block or alert when it detects a GTP-in-GTP message. Upon detection, the firewall generates a GTP log with critical severity. • For 4G and 3G, enable **GTP-U Content Inspection** if you want to inspect and apply policy to the user data payload within a GTP-U packet. Inspecting GTP-U content allows you to correlate IMSI and IMEI information learned from GTP-C messages with the IP traffic encapsulated in GTP-U packets.
5G-C	For 5G, enable **5G-HTTP2** to enable inspection of 5G HTTP/2 control packets, which can contain subscriber IDs, equipment IDs, and network slice information. This enables you to correlate subscriber ID (IMSI), equipment ID (IMEI), and network slice ID information learned from HTTP/2 messages with the IP traffic encapsulated in GTP-U packets. Enabling **5G-HTTP2** disables GTP-C for the profile.
Filtering Options	
RAT Filtering	All Radio Access Technologies (RAT) are allowed by default. GTP-C Create-PDP-Request and Create-Session-Request messages are filtered or allowed based on the RAT filter. You can specify whether to allow, block or alert on the following RAT that the user equipment uses to access the mobile core network: • **UTRAN** • **GERAN** • **WLAN** • **GAN** • **HSPA Evolution** • **EUTRAN** • **Virtual** • **EUTRAN-NB-IoT** • **LTE-M** • **NR** The following RAT are available when enabling **5G-HTTP2**: • **WLAN**

GTP Inspection Profile Settings	
	• **EUTRAN** • **Virtual** • **NR**
IMSI Filtering	IMSI (International Mobile Subscriber Identity) is a unique identification associated with a subscriber in GSM, UMTS and LTE networks that is provisioned in the Subscriber Identity Module (SIM) card. An IMSI is usually presented as a 15-digit number (8 bytes) but can be shorter. IMSI is composed of three parts: • Mobile Country Code (MCC) consisting of three digits. The MCC identifies uniquely the country of domicile of the mobile subscriber. • Mobile Network Code (MNC) consisting of two or three digits; two digits European standard or three digits North American standard. The MNC identifies the home PLMN of the mobile subscriber. • Mobile Subscriber Identification Number (MSIN) identifying the mobile subscriber within a PLMN. The **IMSI Prefix** combines the MCC and MNC and allows you to **allow**, **block**, or **alert** GTP traffic from a specific PLMN. By default all IMSI are allowed. You can either manually enter or import a CSV file with IMSI or IMSI prefixes into the firewall. The IMSI can include wildcards, for example, 310* or 240011*. The firewall supports a maximum of 5,000 IMSI or IMSI prefixes.
APN Filtering	The Access Point Name (APN) is a reference to a GGSN/ PGW that user equipment requires to connect to the internet. In 5G, one format of Data Network Name (DNN) is the APN. The APN is composed of one or two identifiers: • APN Network Identifier that defines the external network to which the GGSN/PGW is connected and optionally a requested service by the mobile station. This part of the APN is mandatory. • APN Operator Identifier that defines in which PLMN GPRS/EPS backbone the GGSN/PGW is located. This part of the APN is optional. All APNs are allowed by default. The APN filter enables you to allow, block, or alert GTP traffic based on the APN value. GTP-C Create-PDP-Request and Create-Session-Request messages are filtered or allowed based on the rules defined for APN filtering. You can manually add or import an APN filtering list into the firewall. The value for the APN must include the network ID or the domain name of the network (for example, example.com) and, optionally, the operator ID. For APN filtering, the wildcard '*' allows you to match for all APN. A combination of '*' and other characters is not supported for wildcards. For example, "internet.mnc* " is treated as a regular APN and will not filter all entries that start with internet.mnc. The firewall supports a maximum of 1,000 APN filters.

GTP Inspection Profile Settings	
GTP Tunnel Limit	
Max Concurrent Tunnels Allowed per Destination	Allows you to limit the maximum number of GTP-U tunnels to a destination IP address, for example to the GGSN (range is 0 to 100,000,000 tunnels)
Alert at Max Concurrent Tunnels per Destination	Specify the threshold at which the firewall triggers an alert when the number of maximum GTP-U tunnels to a destination have been established. A GTP log message of high severity is generated when the configured tunnel limit is reached.
Logging frequency	The number of events that the firewall counts before it generates a log when the configured GTP tunnel limits are exceeded. This setting allows you to reduce the volume to messages logged (range is 0 to 100,000,000; default is 100).
Overbilling Protection	Select the virtual system that serves as the Gi/ SGi firewall on your firewall. The Gi/ SGi firewall inspects the mobile subscriber IP traffic traversing over the Gi/ SGi interface from the PGW/ GGSN to the external PDN (packet data network) such as the internet and secures internet access for mobile subscribers. Overbilling can occur when a GGSN assigns a previously used IP address from the End User IP address pool to a mobile subscriber. When a malicious server on the internet continues to send packets to this IP address as it did not close the session initiated for the previous subscriber and the session is still open on the Gi Firewall. To disallow data from being delivered, whenever a GTP tunnel is deleted (detected by delete-PDP or delete-session message) or timed-out, the firewall enabled for overbilling protection notifies the Gi/ SGi firewall to delete all the sessions that belong to the subscriber from the session table. GTP Security and SGi/ Gi firewall should be configured on the same physical firewall, but can be in different virtual systems. In order to delete sessions based on GTP-C events, the firewall needs to have all the relevant session information and this is possible only when you manage traffic from the SGi + S11 or S5 interfaces for GTPv2 and Gi + Gn interfaces for GTPv1 in the mobile core network.
Other Log Settings By default the firewall does not log allowed GTP messages. You can selectively enable logging of allowed GTP messages for troubleshooting when needed as it will generate high volume of logs. In addition to allowed log messages, this tab also allows you to selectively enable logging of user location information.	
GTPv1-C Allowed Messages	Allows you to selectivity enable logging of the allowed GTPv1-C messages, if you have enabled stateful inspection for GTPv1?C. These messages generate logs to help you troubleshoot issues as needed. By default, the firewall does not log allowed messages. The logging options for allowed GTPv1-C messages are: • **Tunnel Management**—These GTPv1-C messages are used to manage the GTP-U tunnels, which carry encapsulated IP packets and signaling messages between a given pair of network nodes like SGSN and GGSN. It includes messages such as Create PDP Context Request, Create PDP

GTP Inspection Profile Settings	
	Context Response, Update PDP Context Request, Update PDP Context Response, Delete PDP Context Request, Delete PDP Context Response. • **Path Management**—These GTPv1-C messages are typically sent by the GSN or Radio Network Controller (RNC) to the other GSN or RNC to find out if the peer is alive. It includes messages such as Echo Request and Echo Response. • **Others**—These messages include location management, mobility management, RAN information management, and Multimedia Broadcast Multicast Service (MBMS) messages.
Log User Location	Enables you to include the user location information, such as area code and Cell ID, in GTP logs.
Packet Capture	Enables you to capture GTP events.
GTPv2-C Allowed Messages	Enables you to selectively enable logging of the allowed GTPv2-C messages if you enabled stateful inspection for GTPv2-C. These messages generate logs to help you troubleshoot issues as needed. By default, the firewall does not log allowed messages. The logging options for allowed GTPv2-C messages are: • **Tunnel Management**—These GTPv2-C messages are used to manage the GTP-U tunnels, which carry encapsulated IP packets and signaling messages between a given pair of network nodes such as the SGW and PGW. It includes the following types of messages: Create Session Request, Create Session Response, Create Bearer Request, Create Bearer Response, Modify Bearer Request, Modify Bearer Response, Delete Session Request, and Delete Session Response. • **Path Management**—These GTPv2-C messages are typically sent by network node like the SGW or PGW to the other PGW, SGW to find out of the peer is alive. It includes messages such as Echo Request and Echo Response. • **Others**—These messages include mobility management and Non-3GPP access related messages.
GTP-U Allowed Messages	Enables you to selectively enable logging of the allowed GTP-U messages if you enabled stateful inspection for GTPv2-C or GTPv1-C. These messages generate logs to help you troubleshoot issues as needed. The logging options for allowed GTP-U messages are: • **Tunnel Management**—These are GTP-U signaling messages such as Error Indication. • **Path Management**—These GTP-U messages are sent by a network node (such as eNodeB) to another network node (such as SGW) to find out if the peer is alive. It includes messages such as Echo Request/Response. • **G-PDU**—G-PDU (GTP-U PDU) is used for carrying user data packets within the network nodes in the mobile core network; it consists of a GTP header plus a T-PDU.

GTP Inspection Profile Settings	
G-PDU Packets Logged per New GTP-U Tunnel	Enable this option to verify that the firewall is inspecting GTP-U PDUs. The firewall generates a log for the specified number of G-PDU packets in each new GTP-U tunnel (range is 1 to 10; default is 1).
5G-C Allowed Messages	Select **N11** to selectively enable logging of allowed N11 messages. N11 messages help you with troubleshooting and provide deeper visibility into the HTTP/2 messages exchanged over an N11 interface for different procedures. This field is available only if you enabled **5G-HTTP2** on the **5G-C** tab in the Mobile Network Protection profile.

Objects > Security Profiles > SCTP Protection

Create a Stream Control Transmission Protocol (SCTP) Protection profile to specify the ways in which you want the firewall to validate and filter SCTP chunks. You must first enable SCTP Security (**Device** > **Setup** > **Management** > **General Settings**) in order to see this profile type under Security Profiles. You can also limit the number of IP addresses per SCTP endpoint in a multi-homed environment and you can specify when the firewall logs SCTP events. After you create an SCTP Protection profile, you then need to apply the profile to a Security policy rule for a zone.

Firewall models that support SCTP security have a predefined SCTP Protection profile (*default-ss7*) available for you to use as is or you can clone the default-ss7 profile as the foundation for a new SCTP Protection profile. Select **Object** > **Security Profiles** > **SCTP Protection** and select **default-ss7** to see the Operation Codes that cause an alert for this predefined profile.

SCTP Protection Profile Settings	
Name	Enter a name for the SCTP Protection profile.
Description	Enter a description for the SCTP Protection profile.
SCTP Inspection	
Unknown Chunk	Select the firewall action when it receives an SCTP packet with an unknown chunk (the chunk is not defined in RFC3758, RFC4820, RFC4895, RFC4960, RFC5061, or RFC 6525): • **allow** (default)—Allow the packet to pass without modification. • **alert**—Allow the packet to pass without modification and generate an SCTP log (you need to allocate log storage for these logs—see Log Storage tab under Logging and Reporting Settings: Device > Setup > Management). • **block**—Nullify the chunk before passing the packet and generate an SCTP log.
Chunk Flags	Select the firewall action when it receives an SCTP packet with a chunk flag inconsistent with RFC4960: • **allow** (default)—Allow the packet to pass without modification. • **alert**—Allow the packet to pass without modification and generate an SCTP log (you need to allocate log storage for these logs—see Log Storage tab under Logging and Reporting Settings: Device > Setup > Management). • **block**—Drop the packet and generate an SCTP log.
Invalid Length	Select the firewall action when it receives an SCTP chunk with an invalid length: • **allow** (default)—Allow the packet or chunk to pass without modification. • **block**—Drop the packet and generate an SCTP log (you need to allocate log storage for these logs—see Log Storage tab.

SCTP Protection Profile Settings	
IP address limit for multihoming	Enter the maximum number of IP addresses you can configure for an SCTP endpoint before the firewall generates an alert message (range is 1 to 8; default is 4). SCTP multihoming is the ability of an endpoint to support more than one IP address for an association with a peer. If one path to an endpoint fails, SCTP selects one of the other destination IP addresses provided for that association.
Log Settings	Select any combination of settings to generate SCTP logs for allowed chunks, association start and end, and state failure events: • **Log at Association Start** • **Log at Association End** • **Log Allowed Association Initialization Chunks** • **Log Allowed Heartbeat Chunks** • **Log Allowed Association Termination Chunks** • **Log All Control Chunks** • **Log State Failure Events** For the firewall to store SCTP logs, you need to allocate SCTP log storage (see Log Storage tab under Logging and Reporting Settings: Device > Setup > Management).
Filtering Options	
SCTP Filtering	
Name	Enter a name for the SCTP filter.
PPID	Specify a PPID for the SCTP filter: • **any**—causes the firewall to take the Action you specify on all SCTP data chunks containing a PPID. • **3GPP PUA** • **3GPP RNA** • **LCS-AP** • **M2PA** • **M2UA** • **M3UA** • **NBAP** • **RUA** • **S1AP** • **SBc-AP** • **SUA** • **X2AP** • Enter a valid PPID value (one that isn't present in the drop-down). For example, the PPID value for H.323 is 13. Each SCTP filter can specify only one PPID, but you can specify multiple SCTP filters for an SCTP Protection profile.

SCTP Protection Profile Settings	
Action	Specify the action the firewall takes on data chunks containing the specified PPID: • **allow** (default)—Allow the chunk to pass without modification. • **alert**—Allow the chunk to pass without modification and generate an SCTP log (you need to allocate log storage for these logs—see Log Storage tab under Logging and Reporting Settings: Device > Setup > Management). • **block**—Nullify the chunk before passing the packet and generate an SCTP log (you need to allocate log storage for these logs—see Log Storage tab under Logging and Reporting Settings: Device > Setup > Management).
SCTP packets are matched to filters in the list from top to bottom. If you create more than one SCTP filter for a profile, the order of SCTP filters makes a difference. Select a filter and **Move Up** or **Move Down** to change its relative priority in the SCTP Filtering list.	
Diameter Filtering	
Name	Enter a name for the Diameter filter.
Action	Specify the action the firewall takes on Diameter chunks containing the specified Diameter Application IDs, Command Code, and AVPs. If the inspected chunk includes the specified Diameter Application ID *and* any of the specified Diameter Command Codes *and* any of the specified Diameter AVPs, then: • **allow** (default)—Allow the chunk to pass without modification. • **alert**—Allow the chunk to pass without modification and generate an SCTP log (you need to allocate log storage for these logs—see Log Storage tab under Logging and Reporting Settings: Device > Setup > Management). • **block**—Nullify the chunk before passing the packet and generate an SCTP log (you need to allocate log storage for these logs—see Log Storage tab under Logging and Reporting Settings: Device > Setup > Management).
Diameter Application ID	Specify the Diameter Application ID for a chunk on which the firewall takes the specified action. • **any** • **3GPP-Rx** • **3GPP-S6a/S6d** • **3GPP-S6c** • **3GPP-S9** • **3GPP-S13/S13** • **3GPP-Sh** • **Diameter Base Accounting** • **Diameter Common Messages** • **Diameter Credit Control**

SCTP Protection Profile Settings	
	Alternatively, you can enter a numerical value of a Diameter Application ID (the range is from 0 to 4,294,967,295). A Diameter filter can have only one Application ID.
Diameter Command Code	Specify the Diameter Command Codes for a chunk on which the firewall takes the specified action. Select **any**, select one of the Diameter Command Codes from the drop-down, or enter a specific value (the range is from 0 to 16,777,215). The drop-down includes only those command codes that apply to the Diameter Application ID selected. You can add multiple Diameter Command Codes in a Diameter filter.
Diameter AVP	Specify the Diameter Attribute-Value Pair (AVP) codes for a chunk on which the firewall takes the specified action. Enter one or more AVP codes or values (the range is from 1 to 16,777,215).
If you create more than one Diameter filter for a profile, the order of Diameter filters makes a difference. Select a filter and **Move Up** or **Move Down** to adjust its relative priority in the Diameter Filtering list.	
SS7 Filtering	
Name	Enter a name for the SS7 filter.
Action	Specify the action the firewall takes on SS7 chunks containing the specified SS7 filter elements. If the chunk being inspected contains the SCCP Calling Party SSN *and* any of the specified SCCP Calling Party Global Title (GT) values *and* any of the specified Operation Codes, then: • **allow** (default)—Allow the chunk to pass without modification. • **alert**—Allow the chunk to pass without modification and generate an SCTP log (you need to allocate log storage for these logs—see Log Storage tab under Logging and Reporting Settings: Device > Setup > Management). • **block**—Nullify the chunk before passing the packet and generate an SCTP log (you need to allocate log storage for these logs—see Log Storage tab under Logging and Reporting Settings: Device > Setup > Management).
SCCP Calling Party SSN	Specify the SCCP Calling Party SSN for a chunk on which the firewall takes the specified action. Select **any-map** or **Add** one of the SCCP Calling Party SSNs from the drop-down: • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)**

SCTP Protection Profile Settings	
	• **CAP** • **INAP** • **SCCP Management** An SS7 filter can have only one SCCP Calling Party SSN.
SCCP Calling Party GT	Specify the SCCP Calling Party GT value for a chunk on which the firewall takes the specified action. Select **Any** or **Add** a numerical value up to 15 digits. You can also enter a group of SCCP Calling Party GT values using a prefix. For example: 876534*. You can add multiple SCCP Calling Party GT values in an SS7 filter. For SCCP Calling Party SSN: **INAP** and **SCCP Management**, this option is disabled.
Operation Code	Specify the operation code for a chunk on which the firewall takes the specified action: For the following SCCP Calling Party SSNs, select **any**, or an operation code from the drop-down, or enter a specific value (range is 1 to 255): • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** For SCCP Calling Party SSN: **CAP**, enter a value (range is 1 to 255). For SCCP Calling Party SSN: **INAP** and **SCCP Management**, this option is disabled. You can add multiple operation codes in an SS7 filter.
If you create more than one SS7 filter for a profile, the order of SS7 filters makes a difference. Select a filter and **Move Up** or **Move Down** to adjust its relative priority in the SS7 Filtering list.	

Objects > Security Profile Groups

The firewall supports the ability to create Security Profile groups, which specify sets of Security Profiles that can be treated as a unit and then added to security policies. For example, you can create a *threats* Security Profile group that includes profiles for Antivirus, Anti-Spyware, and Vulnerability Protection and then create a Security policy rule that includes the threats profile.

Antivirus, Anti-Spyware, Vulnerability Protection, URL filtering, and file blocking profiles that are often assigned together can be combined into profile groups to simplify the creation of security policies.

To define a new Security Profile, select **Objects** > **Security Profiles**.

The following table describes the Security Profile settings:

Security Profile Group Settings	Description
Name	Enter the profile group name (up to 31 characters). This name appears in the profiles list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared (Panorama only)	Select this option if you want the profile group to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile group will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile group will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this Security Profile group object in device groups that inherit the object. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Profiles	Select an Antivirus, Anti-Spyware, Vulnerability Protection, URL filtering, and/or file blocking profile to be included in this group. Data filtering profiles can also be specified in Security Profile groups. Refer to Objects > Security Profiles > Data Filtering.

Objects > Log Forwarding

By default, the logs that the firewall generates reside only in its local storage. However, you can use Panorama™, the Logging Service, or external services (such as a syslog server) to centrally monitor log information by defining a Log Forwarding profile and assigning that profile to Security, Authentication, DoS Protection, and Tunnel Inspection policy rules. Log Forwarding profiles define forwarding destinations for the following Log Types: Authentication, Data Filtering, GTP, SCTP, Threat, Traffic, Tunnel, URL Filtering, and WildFire® Submissions logs.

You should forward logs to Panorama or to external storage for many reasons, including: compliance, redundancy, running analytics, centralized monitoring, and reviewing threat behaviors and long-term patterns. In addition, the firewall has limited log storage capacity and deletes the oldest logs as when the storage space fills up. Be sure to forward Threat logs and WildFire logs.

To forward other log types, see Device > Log Settings.

To enable a PA-7000 Series firewall to forward logs or forward files to WildFire®, you must first configure a Log Card Interface on the PA-7000 Series firewall. As soon as you configure this interface, the firewall will automatically use this port—there is no special configuration required. Just configure a data port on one of the PA-7000 Series Network Processing Cards (NPCs) as a Log Card interface type and ensure that the network that you use can communicate with your log servers. For WildFire forwarding, the network must communicate successfully with the WildFire cloud or WildFire appliance (or both).

The following table describes the Log Forwarding profile settings.

Log Forwarding Profile Settings	Description
Name	Enter a name (up to 64 characters) to identify the profile. This name appears in the list of Log Forwarding profiles when defining Security policy rules. The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores.
Shared (Panorama only)	Select this option if you want the profile to be available to: • **Every virtual system (vsys) on a multi-vsys firewall**—If you disable (clear) this option, the profile is available only to the **Virtual System** selected in the **Objects** tab. • **Every device group on Panorama**—If you disable (clear) this option, the profile is available only to the **Device Group** selected in the **Objects** tab.
Enable enhanced application logging to Cortex Data Lake (including traffic and url logs) (Panorama only)	Enhanced Application Logs for Palo Alto Networks Cloud Services is available with a Cortex Data Lake subscription. Enhanced application logging allows the firewall to collect data specifically intended to increase visibility into network activity for apps running in the Palo Alto Networks Cloud Services environment.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this Log Forwarding profile in device groups that inherit the profile. This

Log Forwarding Profile Settings	Description
	selection is disabled (cleared) by default, which means administrators can override the settings for any device group that inherits the profile.
Description	Enter a description to explain the purpose of this Log Forwarding profile.
Match List (unlabeled)	**Add** one or more match list profiles (up to 64) that specify forwarding destinations, log attribute-based filters to control which logs the firewall forwards, and actions to perform on the logs (such as automatic tagging). Complete the following two fields (Name and Description) for each match list profile.
Name (match list profile)	Enter a name (up to 31 characters) to identify the match list profile.
Description (match list profile)	Enter a description (up to 1,023 characters) to explain the purpose of this match list profile.
Log Type	Select the type of logs to which this match list profile applies: authentication (**auth**), **data**, **gtp**, **sctp**, **threat**, **traffic**, **tunnel**, **URL**, or **WildFire**.
Filter	By default, the firewall forwards **All Logs** of the selected **Log Type**. To forward a subset of the logs, select an existing filter from the drop-down or select **Filter Builder** to add a new filter. For each query in a new filter, specify the following fields and **Add** the query: • **Connector**—Select the connector logic (and/or) for the query. Select **Negate** if you want to apply negation to the logic. For example, to avoid forwarding logs from an untrusted zone, select **Negate**, select **Zone** as the Attribute, select **equal** as the Operator, and enter the name of the untrusted Zone in the Value column. • **Attribute**—Select a log attribute. The available attributes depend on the **Log Type**. • **Operator**—Select the criterion to determine whether the attribute applies (such as **equal**). The available criteria depend on the **Log Type**. • **Value**—Specify the attribute value to match. To display or export the logs that the filter matches, **View Filtered Logs**, which provides the same options as the **Monitoring** tab pages (such as **Monitoring** > **Logs** > **Traffic**).
Panorama Panorama/Logging Service (Panorama only)	Select **Panorama** if you want to forward logs to Log Collectors or the Panorama management server or to forward logs to the Logging Service. If you enable this option, you must configure log forwarding to Panorama. To use the Logging Service, you must also **Enable** the Logging Service in Device > Setup > Management.
SNMP	**Add** one or more SNMP Trap server profiles to forward logs as SNMP traps (see Device > Server Profiles > SNMP Trap).
Email	**Add** one or more Email server profiles to forward logs as email notifications (see Device > Server Profiles > Email).

Log Forwarding Profile Settings	Description
Syslog	**Add** one or more Syslog server profiles to forward logs as syslog messages (see Device > Server Profiles > Syslog).
HTTP	**Add** one or more HTTP server profiles to forward logs as HTTP requests (see Device > Server Profiles > HTTP).
Built-in Actions	You can select from two types of built-in actions when you **Add** an action to perform—Tagging and Integration. • **Tagging**—Add or remove a tag to the source or destination IP address in a log entry automatically and register the IP address and tag mapping to a User-ID agent on the firewall or Panorama, or to a remote User-ID agent so that you can respond to an event and dynamically enforce Security policy. The ability to tag an IP address and dynamically enforce policy using dynamic address groups gives you better visibility, context, and control for consistently enforcing Security policy irrespective of where the IP address moves across your network. Configure the following settings: • **Add** an action and enter a name to describe it. • Select the target IP address you want to tag—**Source Address** or **Destination Address**. You can take an action for all log types that include a source or destination IP address in the log entry. You can tag the source IP address only, in Correlation logs and HIP Match logs; you cannot configure an action for System logs and Configuration logs because the log type does not include an IP address in the log entry. • Select the action—**Add Tag** or **Remove Tag**. • Select whether to register the IP address and tag mapping to the **Local User-ID** agent on this firewall or Panorama, or to a **Remote User-ID** agent. • To register the IP address and tag mapping to a **Remote User-ID** agent, select the HTTP server profile (Device > Server Profiles > HTTP) that will enable forwarding. • Configure the IP-Tag **Timeout** to set, in minutes, the amount of time that IP address-to-tag mapping is maintained. Setting the timeout to 0 means that the IP-Tag mapping does not timeout (range is 0 to 43200 (30 days); default is 0). *You can only configure a timeout with the Add Tag action.* • Enter or select the **Tags** you want to apply or remove from the target source or destination IP address. • **Integration**—Only available on the VM-Series firewall on Azure. This option allows you to forward the selected logs to the Azure Security Center using the **Azure-Security-Center-Integration** action. To add a device to the quarantine list based on the log forwarding profile filter, select **Quarantine**.

Objects > Authentication

An authentication enforcement object specifies the method and service to use for authenticating end users who access your network resources. You assign the object to Authentication policy rules, which invoke the authentication method and service when traffic matches a rule (see Policies > Authentication).

The firewall has the following predefined, read-only authentication enforcement objects:

- **default-browser-challenge**—The firewall transparently obtains user authentication credentials. If you select this action, you must enable Kerberos Single Sign-On (SSO) or NT LAN Manager (NTLM) authentication when you configure Authentication Portal. If Kerberos SSO authentication fails, the firewall falls back to NTLM authentication. If you did not configure NTLM, or NTLM authentication fails, the firewall falls back to the authentication method specified in the predefined **default-web-form** object.
- **default-web-form**—To authenticate users, the firewall uses the certificate profile or authentication profile you specified when configuring Authentication Portal. If you specified an authentication profile, the firewall ignores any Kerberos SSO settings in the profile and presents an Authentication Portal page for the user to enter authentication credentials.
- **default-no-captive-portal**—The firewall evaluates Security policy without authenticating users.

Before creating a custom authentication enforcement object:

- Configure a server profile that specifies how to connect to the authentication service (see Device > Server Profiles).
- Assign the server profile to an authentication profile that specifies authentication settings such as Kerberos single sign-on parameters (see Device > Authentication Profile).

To create a custom authentication enforcement object, click **Add** and complete the following fields:

Authentication Enforcement Settings	Description
Name	Enter a descriptive name (up to 31 characters) to help you identify the object when defining Authentication rules. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared (Panorama only)	Select this option if you want the object to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the object will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the object will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this authentication enforcement object in device groups that inherit the object. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Authentication Method	Select a method: • **browser-challenge**—The firewall transparently obtains user authentication credentials. If you select this action, the **Authentication Profile** you select must have Kerberos SSO enabled.

Authentication Enforcement Settings	Description
	• **web-form**—To authenticate users, the firewall uses the certificate profile you specified when configuring Authentication Portal or the **Authentication Profile** you select in the authentication enforcement object. If you select an **Authentication Profile**, the firewall ignores any Kerberos SSO settings in the profile and presents an Authentication Portal page for the user to enter authentication credentials. • **no-captive-portal**—The firewall evaluates Security policy without authenticating users.
Authentication Profile	Select the authentication profile that specifies the service to use for validating the identities of users.
Message	Enter instructions that tell users how to respond to the first authentication challenge that they see when their traffic triggers the Authentication rule. The message displays in the **Authentication Portal Comfort Page**. If you don't enter a message, the default **Authentication Portal Comfort Page** displays (see Device > Response Pages).  *The firewall displays the Authentication Portal Comfort Page only for the first authentication challenge (factor), which you define in the Authentication tab of the Authentication Profile (see Device > Authentication Profile). For multi-factor authentication (MFA) challenges that you define in the Factors tab of the profile, the firewall displays the MFA Login Page.*

Objects > Decryption Profile

Decryption profiles enable you to block and control specific aspects of SSL and SSH traffic that you have specified for decryption, as well as traffic that you have explicitly excluded from decryption. After you create a decryption profile, you can then add that profile to a decryption policy; any traffic matched to the decryption policy is additionally enforced based on the profile settings.

A default decryption profile is configured on the firewall, and is automatically included in new decryption policies (you cannot modify the default decryption profile). Click **Add** to create a new decryption profile, or select an existing profile to **Clone** or modify it.

What are you looking for?	See:
Add a new decryption profile. Enable port mirroring for decrypted traffic.	Decryption Profile General Settings
Block and control SSL decrypted traffic.	Settings to Control Decrypted SSL Traffic
Block and control traffic that you have excluded from decryption (for example, traffic classified as health and medicine or financial services).	Settings to Control Traffic that is not Decrypted
Block and control decrypted SSH traffic.	Settings to Control Decrypted SSH Traffic

Decryption Profile General Settings

The following table describes the general settings for decryption profiles.

Decryption Profile — General Settings	Description
Name	Enter a profile name (up to **31** characters). This name appears in the list of decryption profiles when defining decryption policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared (Panorama only)	Select this option if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this Decryption profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.

Decryption Profile — General Settings	Description
Decryption Mirroring Interface (Supported on all models except the VM-Series firewall on AWS, Azure, NSX edition, and Citrix SDX.)	Select an **Interface** to use for decryption port mirroring. *Before you can enable decryption port mirroring, you must obtain a Decryption Port Mirror license, install the license, and reboot the firewall.*
Forwarded Only (Supported on all models except the VM-Series firewall on AWS, Azure, NSX edition, and Citrix SDX.)	Select **Forwarded Only** if you want to mirror decrypted traffic only after Security policy enforcement. With this option, only traffic that is forwarded through the firewall is mirrored. This option is useful if you are forwarding the decrypted traffic to other threat detection devices, such as a DLP device or another intrusion prevention system (IPS). If you clear this selection (the default setting), the firewall will mirror all decrypted traffic to the interface before security policies lookup, which allows you to replay events and analyze traffic that generates a threat or triggers a drop action.

Settings to Control Decrypted Traffic

The following table describes the settings you can use to control traffic that the firewall decrypted using either Forward Proxy decryption or Inbound Inspection (including the SSL Protocol Settings tab). You can use these settings to limit or block TLS sessions based on criteria including the status of the external server certificate, the use of unsupported cipher suites or protocol versions, or the availability of system resources to process decryption.

SSL Decryption Tab Settings	Description
SSL FORWARD PROXY TAB Select options to limit or block TLS traffic decrypted using Forward Proxy.	
Server Certificate Validation—Select options to control server certificates for decrypted traffic.	
Block sessions with expired certificates	Terminate the TLS connection if the server certificate is expired. This prevents users from accepting expired certificates and continuing with an TLS session. *Block sessions with expired certificates to prevent access to potentially insecure sites.*
Block sessions with untrusted issuers	Terminate the TLS session if the server certificate issuer is untrusted. *Block sessions with untrusted issuers because an untrusted issuer may indicate a man-in-the-middle attack, a replay attack, or another attack.*

SSL Decryption Tab Settings	Description
Block sessions with unknown certificate status	Terminate the TLS session if a server returns a certificate revocation status of “unknown”. Certificate revocation status indicates if trust for the certificate has been or has not been revoked.  *Block sessions with unknown certificate status for the tightest security. However, because certificate status may be unknown for a variety of reasons, this may tighten security too much. If blocking unknown certificate status affects sites you need to use for business, don’t block sessions with unknown certificate status.*
Block sessions on the certificate status check timeout	Terminate the TLS session if the certificate status cannot be retrieved within the amount of time that the firewall is configured to stop waiting for a response from a certificate status service. You can configure **Certificate Status Timeout** value when creating or modifying a certificate profile (**Device** > **Certificate Management** > **Certificate Profile**). Blocking sessions when the status check times out is a tradeoff between tighter security and a better user experience. If certificate revocation servers respond slowly, blocking on a timeout may block sites that have valid certificates. You can increase the timeout value for Certificate Revocation Checking (CRL) and Online Certificate Status Protocol (OCSP) if you are concerned about timing out valid certificates.
Restrict certificate extensions	Limits the certificate extensions used in the dynamic server certificate to key usage and extended key usage.  *Restrict certificate extensions if your deployment requires no other certificate extensions.*
Append certificate's CN value to SAN extension	Enable the firewall to add a Subject Alternative Name (SAN) extension to the impersonation certificate it presents to clients as part of Forward Proxy decryption. When a server certificate contains only a Common Name (CN), the firewall adds a SAN extension to the impersonation certificate based on the server certificate CN. This option is useful in cases where browsers require server certificates to use a SAN and no longer support certificate matching based on CNs; it ensures that end users can continue to access their requested web resources and that the firewall can continue to decrypt sessions even if a server certificate contains only a CN.  *Append the certificate’s CN value to the SAN extension to help ensure access to requested web resources.*
Unsupported Mode Checks—Select options to control unsupported TLS applications.	
Block sessions with unsupported versions	Terminate sessions if PAN-OS does not support the “client hello” message. PAN-OS supports SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3.

SSL Decryption Tab Settings	Description
	Always block sessions with unsupported versions to prevent access to sites with weak protocols. On the SSL Protocol Settings tab, set the minimum Protocol Version to TLSv1.2 to block sites with weak protocol versions. If a site you need to access for business purposes uses a weaker protocol, create a separate Decryption profile that allows the weaker protocol and specify it in a Decryption policy rule that applies only to the sites for which you must allow the weaker protocol.
Block sessions with unsupported cipher suites	Terminate the session if the cipher suite specified in the TLS handshake if it is not supported by PAN-OS. *Block sessions that use cipher suites you don't support. You configure which cipher suites (encryption algorithms) to allow on the SSL Protocol Settings tab. Don't allow users to connect to sites with weak cipher suites.*
Block sessions with client authentication	Terminate sessions with client authentication for Forward Proxy traffic. *Block sessions with client authentication unless an important application requires it, in which case you should create a separate Decryption profile and apply it only to traffic that requires client authentication.*
Failure Checks—Select the action to take if system resources are not available to process decryption.	
Block sessions if resources not available	Terminate sessions if system resources are not available to process decryption. Whether to block sessions when resources aren't available is a tradeoff between tighter security and a better user experience. If you don't block sessions when resources aren't available, the firewall won't be able to decrypt traffic that you want to decrypt when resources are impacted. However, blocking sessions when resources aren't available may affect the user experience because sites that are normally reachable may become temporarily unreachable.
Block sessions if HSM not available	Terminate sessions if a hardware security module (HSM) is not available to sign certificates. Whether to block sessions if the HSM isn't available depends on your compliance rules about where private keys must come from and how you want to handle encrypted traffic if the HSM isn't available.
Block downgrade on no resources	Terminate the session if system resources are not available to process the TLSv1.3 handshake (instead of downgrading to TLSv1.2). Whether to block sessions when resources aren't available is a tradeoff between tighter security and a better user experience. If you block downgrading the handshake to TLSv1.2 when TLSv1.3 resources aren't available, the firewall drops the session. If you do not block

SSL Decryption Tab Settings	Description
	downgrading the handshake, then if resources aren't available for the TLSv1.3 handshake, the firewall downgrades to TLSv1.2.
Client Extension	
Strip ALPN	The firewall processes and inspects HTTP/2 traffic by default. However, you can disable HTTP/2 inspection by specifying for the firewall to **Strip ALPN**. With this option selected, the firewall removes any value contained in the Application-Layer Protocol Negotiation (ALPN) TLS extension). Because ALPN is used to secure HTTP/2 connections, when there is no value specified for this TLS extension, the firewall either downgrades HTTP/2 traffic to HTTP/1.1 or classifies it as unknown TCP traffic.

For unsupported modes and failure modes, the session information is cached for 12 hours, so future sessions between the same hosts and server pair are not decrypted. Enable the options to block those sessions instead.

SSL INBOUND INSPECTION TAB

Select options to limit or block traffic decrypted using Inbound Inspection.

Unsupported Mode Checks—Select options to control sessions if unsupported modes are detected in TLS traffic.

Block sessions with unsupported versions	Terminate sessions if PAN-OS does not support the "client hello" message. PAN-OS supports SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3. *Always block sessions with unsupported versions to prevent access to sites with weak protocols. On the SSL Protocol Settings tab, set the minimum Protocol Version to TLSv1.2 to block sites with weak protocol versions. If a site you need to access for business purposes uses a weaker protocol, create a separate Decryption profile that allows the weaker protocol and specify it in a Decryption policy rule that applies only to the sites for which you must allow the weaker protocol.*
Block sessions with unsupported cipher suites	Terminate the session if the cipher suite used is not supported by PAN-OS. *Block sessions that use cipher suites you don't support. You configure which cipher suites (encryption algorithms) to allow on the SSL Protocol Settings tab. Don't allow users to connect to sites with weak cipher suites.*

Failure Checks—Select the action to take if system resources are not available.

Block sessions if resources not available	Terminate sessions if system resources are not available to process decryption.

SSL Decryption Tab Settings	Description
	Whether to block sessions when resources aren't available is a tradeoff between tighter security and a better user experience. If you don't block sessions when resources aren't available, the firewall won't be able to decrypt traffic that you want to decrypt when resources are impacted. However, blocking sessions when resources aren't available may affect the user experience because sites that are normally reachable may become temporarily unreachable.
Block sessions if HSM not available	Terminate sessions if a hardware security module (HSM) is not available to decrypt the session key. Whether to block sessions if the HSM isn't available depends on your compliance rules about where private keys must come from and how you want to handle encrypted traffic if the HSM isn't available.
Block downgrade on no resources	Terminate the session if system resources are not available to process the TLSv1.3 handshake (instead of downgrading to TLSv1.2). Whether to block sessions when resources aren't available is a tradeoff between tighter security and a better user experience. If you block downgrading the handshake to TLSv1.2 when TLSv1.3 resources aren't available, the firewall drops the session. If you do not block downgrading the handshake, then if resources aren't available for the TLSv1.3 handshake, the firewall downgrades to TLSv1.2.
SSL PROTOCOL SETTINGS TAB Select the following settings to enforce protocol versions and cipher suites for TLS session traffic.	
Protocol Versions	Enforce the use of minimum and maximum protocol versions for the TLS session.
Min Version	Set the minimum protocol version that can be used to establish the TLS connection. *Set the Min Version to TLSv1.2 to provide the strongest security. Review sites that don't support TLSv1.2 to see if they really have a legitimate business purpose. For sites you need to access that don't support TLSv1.2, create a separate Decryption profile that specifies the strongest protocol version they support and apply it to a Decryption policy rule that limits the use of the weak version to only the necessary sites, from only the necessary sources (zones, addresses, users).*
Max Version	Set the maximum protocol version that can be used to establish the TLS connection. You can choose the option Max so that no maximum version is specified; in this case, protocol versions that are equivalent to or are a later version than the selected minimum version are supported. *Set the Max Version to Max so that as protocols improve, the firewall automatically supports them.*

SSL Decryption Tab Settings	Description
	However, if your Decryption policy supports mobile applications, many of which use pinned certificates, set the Max Version to TLSv1.2. Because TLSv1.3 encrypts certificate information that was not encrypted in previous TLS versions, the firewall can't automatically add decryption exclusions based on certificate information, which affects some mobile applications. Therefore, if you enable TLSv1.3, the firewall may drop some mobile application traffic unless you create a No Decryption policy for that traffic. If you know the mobile applications you use for business, consider creating a separate Decryption policy and profile for those applications so that you can enable TLSv1.3 for all other traffic.
Key Exchange Algorithms	Enforce the use of the selected key exchange algorithms for the TLS session. All three algorithms (**RSA**, **DHE**, and **ECDHE**) are enabled by default. The **DHE** (Diffie-Hellman) and **ECDHE** (elliptic curve Diffie-Hellman) enable Perfect Forward Secrecy (PFS) for Forward Proxy or Inbound Inspection decryption.
Encryption Algorithms	Enforce the use of the selected encryption algorithms for the TLS session.  *Don't support the weak 3DES or RC4 encryption algorithms. (The firewall automatically blocks these two algorithms when you use TLSv1.2 or greater as the minimum protocol version.) If you have to make an exception and support a weaker protocol version, uncheck 3DES and RC4 in the Decryption profile. If there are sites you must access for business purposes that use 3DES or RC4 encryption algorithms, create a separate Decryption profile and apply it to a Decryption policy rule for just those sites.*
Authentication Algorithms	Enforce the use of the selected authentication algorithms for the TLS session.  *Block the old, weak MD5 algorithm (blocked by default). If no necessary sites use SHA1 authentication, block SHA1. If any sites you require for business purposes use SHA1, create a separate Decryption profile and apply it to a Decryption policy rule for just those sites.*

Settings to Control Traffic that is not Decrypted

You can use the **No Decryption** tab to enable settings to block traffic that is matched to a decryption policy configured with the **No Decrypt** action (**Policies** > **Decryption** > **Action**). Use these options to control server certificates for the session, though the firewall does not decrypt and inspect the session traffic.

No Decryption Tab Settings	Description
Block sessions with expired certificates	Terminate the SSL connection if the server certificate is expired. This prevents users from accepting expired certificates and continuing with an SSL session.  *Block sessions with expired certificates to prevent access to potentially insecure sites.*
Block sessions with untrusted issuers	Terminate the SSL session if the server certificate issuer is untrusted.  *Block sessions with untrusted issuers because an untrusted issuer may indicate a man-in-the-middle attack, a replay attack, or another attack.*

Settings to Control Decrypted SSH Traffic

The following table describes the settings you can use to control decrypted inbound and outbound SSH traffic. These settings allow you to limit or block SSH tunneled traffic based on criteria including the use of unsupported algorithms, the detection of SSH errors, or the availability of resources to process SSH Proxy decryption.

SSH Proxy Tab Settings	Description
Unsupported Mode Checks—Use these options to control sessions if unsupported modes are detected in SSH traffic. Supported SSH version is SSH version 2.	
Block sessions with unsupported versions	Terminate sessions if the “client hello” message is not supported by PAN-OS.  *Always block sessions with unsupported versions to prevent access to sites with weak protocols. On the SSL Protocol Settings tab, set the minimum Protocol Version to TLSv1.2 to block sites with weak protocol versions. If a site you need to access for business purposes uses a weaker protocol, create a separate Decryption profile that allows the weaker protocol and specify it in a Decryption policy rule that applies only to the sites for which you must allow the weaker protocol.*
Block sessions with unsupported algorithms	Terminate sessions if the algorithm specified by the client or server is not supported by PAN-OS.  *Always block sessions with unsupported algorithms to prevent access to sites that use weak algorithms.*
Failure Checks—Select actions to take if SSH application errors occur and if system resources are not available.	

SSH Proxy Tab Settings	Description
Block sessions on SSH errors	Terminate sessions if SSH errors occur.
Block sessions if resources not available	Terminate sessions if system resources are not available to process decryption. Whether to block sessions when resources aren't available is a tradeoff between tighter security and a better user experience. If you don't block sessions when resources aren't available, the firewall won't be able to decrypt traffic that you want to decrypt when resources are impacted. However, blocking sessions when resources aren't available may affect the user experience because sites that are normally reachable may become temporarily unreachable.

Objects > Decryption > Forwarding Profile

You can set up a Decryption Forwarding profile to enable the firewall to act as a decryption broker. A decryption broker firewall forwards traffic that it has already decrypted and inspected to a security chain—a set of inline, third-party security appliances—for additional enforcement. You can also configure the firewall to provide session distribution for the security chain to ensure that security-chain devices are not oversubscribed. When the firewall receives traffic back from the security chain, the firewall re-encrypts the traffic and forwards it to the appropriate destination.

Before you create a Decryption Forwarding profile to enable decryption brokering, you must:

- Enable SSL Forward Proxy decryption.
- Dedicate at least two Layer 3 interfaces on the firewall for forwarding decrypted traffic to the security chain (select **Network** > **Interfaces** > **Ethernet**, edit an interface, select **Advanced** > **Other Info**, and then enable Decrypt Forward). Repeat this task to enable a second interface as a Decrypt Forward interface.

After you complete these tasks, create a Decryption Forwarding profile to pair the two interfaces and define settings for the security chain to which the firewall will forward decrypted traffic.

See Decryption Broker to learn more about supported decryption broker and security chain deployments and for the full workflow to enable a firewall to act as a decryption broker.

Decryption Forwarding Settings	Description
Name	Give the profile a descriptive name.
Description	Optionally describe the profile settings.
General Tab	
Security Chain Type	Select the type of security chain to which the firewall forwards decrypted traffic: • **Routed (Layer 3)**: The devices in this type of security chain use Layer 3 interfaces to connect to the security-chain network—each interface must have an assigned IP address and subnet mask. Security-chain devices are configured with static routes (or dynamic routing) to direct inbound and outbound traffic to the next device in the security chain and back to the firewall. • **Transparent Bridge**: In a transparent-bridge security-chain network, all security-chain devices are configured with two interfaces connected to the security-chain network. These two dataplane interfaces are configured to be in Transparent Bridge mode; they do not have assigned IP addresses, subnet masks, default gateways, or local routing tables. Security-chain devices in Transparent Bridge mode receive traffic on one interface and then analyze and enforce the traffic before it egresses the other interface on the way to the next inline security-chain device.
Flow Direction	Specify how the firewall directs decrypted inbound and outbound sessions through a security chain: in the same direction (unidirectionally) or in opposite directions (bidirectionally). The flow direction you choose depends on the type of devices that make up your security chain. For example, if a

Decryption Forwarding Settings	Description
	security chain comprises of stateless devices that can examine both sides of a session, you would choose a unidirectional flow.
Primary Interface Secondary Interface	Select the primary and secondary interfaces that the firewall will use to forward traffic to a security chain. Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you configure as Decrypt Forward interfaces are displayed.
Security Chains Tab	
Enable	Enable the security chain.
Name	Give the security chain a descriptive name.
First Device Last Device	Select the IPv4 address of the first device and the last device in the security chain or define a new Address Object to easily reference the device.
Session Distribution Method	When forwarding to multiple Routed (Layer 3) security chains, choose the method that the firewall will use to distribute decrypted sessions among security chains: • **IP Modulo**—The firewall assigns sessions based on the module hash of the source and destination IP addresses. • **IP Hash**—The firewall assigns sessions based on the IP hash of the source and destination IP addresses and port numbers. • **Round Robin**—The firewall allocates sessions evenly among security chains. • **Lowest Latency**—The firewall allocates more sessions to the security chain with the lowest latency. For this method to work as expected, you must also enable Latency Monitoring and HTTP Monitoring (select **Health Monitor**).
Health Monitor Tab	
On Health Check Failure	Choose for the firewall to either **Bypass Security Chain** (allow session traffic) or **Block Session** if all security chains associated with this decryption forwarding profile fail a health check. This means that when a decryption profile is configured with multiple security chains, if a single security chain fails a health check, the firewall performs session distribution across the remaining healthy security chains based on the method specified on the **Security Chains** tab—it only blocks or allow the traffic based on this setting in the event that every security chain fails.
Health Check Failed Condition	Define a health check failure as an event where any of the health monitor conditions are met (an **OR Condition**) or when all of the conditions are met (an **AND Condition**).
Path Monitoring	Enable path, latency, or HTTP monitoring or any combination of the three to identify when security chains are not effectively processing decrypted

Decryption Forwarding Settings	Description
Latency Monitoring	traffic. For each type of monitoring you enable, define the periods of time and counts that will trigger a health check failure.
HTTP Monitoring	Enable: • Path monitoring to check device connectivity. • Latency monitoring to check device processing speed and efficiency. • HTTP monitoring to check device availability and response time.

Objects > SD-WAN Link Management

Create profiles to apply to sets of applications and services specified in SD-WAN policy rules. Each profile type controls various aspects of SD-WAN link management.

- Objects > SD-WAN Link Management > Path Quality Profile
- Objects > SD-WAN Link Management > SaaS Quality Profile
- Objects > SD-WAN Link Management > Traffic Distribution Profile
- Objects > SD-WAN Link Management > Error Correction Profile

Objects > SD-WAN Link Management > Path Quality Profile

SD-WAN allows you to create a path quality profile for each set of applications, application filters, application groups, services, service objects, and service group objects that has unique network quality requirements and reference the profile in an SD-WAN policy rule. In the profile you set maximum thresholds for three parameters: latency, jitter, and packet loss. When an SD-WAN link exceeds any one of the thresholds, the firewall selects a new best path for packets matching the SD-WAN rule where you apply this profile.

The sensitivity setting for each path quality parameter allows you to indicate to the firewall which parameter is more important (preferred) for the application(s) to which the profile applies. The firewall places more importance on a parameter with a high setting than a parameter with a medium or low setting. For example, some applications are more sensitive to packet loss than to jitter or latency, so you could set packet loss to high sensitivity, which causes the firewall to examine packet loss first.

If you let the sensitivity settings for latency, jitter, and packet loss remain at the default setting (medium) or if you set all three parameters to the same setting, the order of preference for the profile is packet loss, latency, jitter.

By default, the firewall measures latency and jitter every 200ms and takes an average of the last three measurements to measure path quality in a sliding window. You can modify this behavior by selecting aggressive or relaxed path monitoring when you configure an SD-WAN Interface Profile.

	Path Quality Profile Settings
Name	Enter a name for the path quality profile using a maximum of 31 alphanumeric characters, underscore, hyphen, space, and period.
Latency (ms)	**Threshold**—Enter the number of milliseconds allowed for a packet to leave the firewall, arrive at the opposite end of the SD-WAN tunnel, and a response packet to return to the firewall before the threshold is exceeded (range is 10 to 2,000; default is 100).
	Sensitivity—Select **high**, **medium**, or **low** (default is **medium**).
Jitter (ms)	**Threshold**—Enter the number of milliseconds (range is 10 to 1,000; default is 100).
	Sensitivity—Select **high**, **medium**, or **low** (default is **medium**).
Packet Loss (%)	**Threshold**—Enter the percentage of packets lost on the link before the threshold is exceeded (range is 1 to 100.0; default is 1).

	Path Quality Profile Settings
	Sensitivity—The Sensitivity setting for Packet Loss has no effect, so leave the default setting (**medium**).

Objects > SD-WAN Link Management > SaaS Quality Profile

SD-WAN allows you to create Software-as-a-Service (SaaS) quality profile to measure the path health quality between your hub or branch firewall and a server-side SaaS applications in order to accurately monitor SaaS application reliability and swap paths should the path health quality degrade. This allows the firewall to accurately determine when to failover to a different Direct Internet Access (DIA) link.

The SaaS quality profile allows you to specify the SaaS application to monitor using an adaptive learning algorithm that monitors the application activity, or by specifying a SaaS application using the application IP address, FQDN, or URL.

	SaaS Quality Profile Settings
Name	Enter a name for the path quality profile using alphanumeric characters, underscore, hyphen, space, and period.
Shared (Panorama only)	Check (enable) to make the SaaS Quality profile shared across all device groups.
Disable Override (Panorama only)	Check (enable) to disable the ability to override the SaaS Quality profile settings locally on the managed firewall.
SaaS Monitoring Mode	
Adaptive	The SaaS application session activity is monitored for send and receive activity and the path health status is derived automatically without any additional health checks on the SD-WAN interface. This option is selected by default.
Static IP Address	**IP Address/Object**—Specify the SaaS application to monitor using the application IP address. • **IP Address**— The IP address of the SaaS application. • **Probe Interval (Sec)**—Specify, in seconds, the interval the firewall probes the path quality health between the firewall and the SaaS application. Default is 3 seconds. Up to 4 static IP addresses are supported.
	FQDN—Specify the SaaS application to monitor using the application Fully Qualified Domain Name (FQDN). • **FQDN**— The FQDN of the SaaS application. You must configure a FQDN address object to specify a FQDN. The SaaS application FQDN must be resolvable in order to successfully monitor the SaaS application.

	SaaS Quality Profile Settings
	• **Probe Interval (sec)**—Specify, in seconds, the interval the firewall probes the path quality health between the branch firewall and the SaaS application. Default is 3 seconds.
HTTP/HTTPS	Specify the SaaS application to monitor using the HTTP or HTTPS URL. • **Monitored URL**—The HTTP or HTTPS URL of the SaaS application. • **Probe Interval (sec)**—Specify, in seconds, the interval the firewall probes the path quality health between the firewall and the SaaS application. Default is 3 seconds.

Objects > SD-WAN Link Management > Traffic Distribution-Profile

For this Traffic Distribution profile, select the method the firewall uses to distribute sessions and to fail over to a better path when path quality deteriorates. Add the Link Tags that the firewall considers when determining the link on which it forwards SD-WAN traffic. You apply a Traffic Distribution profile to each SD-WAN policy rule you create.

	Traffic Distribution Profile
Name	Enter a name for the Traffic Distribution Profile using a maximum of 31 alphanumeric characters, hyphen, space, underscore, and period.
Best Available Path	If cost is not a factor and you will allow applications to use any path out of the branch, select Best Available Path. The firewall distributes traffic and fails over to a link from among the links belonging to all the Link Tags in the list based path quality metrics to provide the best application experience to users.
Top Down Priority	If you have expensive or low capacity links that you want to use only as a last resort or as a backup link, select the Top Down Priority method and place the tags that include those links last in the list of Link Tags for this profile. The firewall uses the top Link Tag in the list first to determine the links on which to session load traffic and on which to fail over. If none of the links in the top Link Tag are qualified, the firewall selects a link from the second Link Tag in the list. If none of the links in the second Link Tag are qualified, the process continues as necessary until the firewall finds a qualified link in the last Link Tag. If all associated links are overloaded and no link meets quality thresholds, the firewall uses the Best Available Path method to select a link on which to forward traffic. If the application's jitter, latency, or packet loss exceeds its configured threshold, the firewall starts at the top of the Top Down list of Link Tags to find a link to which it fails over.
Weighted Session Distribution	Select Weighted Session Distribution if you want to manually load traffic (that matches the rule) onto your ISP and WAN links and you don't require failover during brownout conditions. You manually specify the link's load when you apply a static percentage of new sessions that the interfaces grouped with a single tag will get. You might select this method for applications that aren't sensitive to latency and that require a lot of the link's bandwidth capacity, such as large branch backups and

	Traffic Distribution Profile
	large file transfers. Keep in mind that if the link experiences brownout, the firewall doesn't reflect the matching traffic to a different link.
Link Tags	Add the Link Tags you want the firewall to consider during the link selection process you chose for this profile. The order of tags matters if you chose the Top Down Priority method; use Move Up or Move Down to change the order of tags.
Weight	If you chose the Weighted Session Distribution method, enter a percentage for each Link Tag you added. The sum of the percentage values must equal 100%.

Objects > SD-WAN Link Management > Error Correction Profile

If your SD-WAN traffic includes an application that is sensitive to packet loss or corruption, such as audio, VoIP, or video conferencing, you can apply either Forward Error Correction (FEC) or packet duplication as a means of error correction. With FEC, the receiving firewall (decoder) can recover lost or corrupted packets by employing parity bits that the encoder embeds in an application flow. Packet duplication is an alternative method of error correction, in which an application session is duplicated from one tunnel to a second tunnel. Both methods require additional bandwidth and CPU overhead; therefore, apply FEC or packet duplication only to applications that can benefit from such a method. To employ one of these methods, create an Error Correction Profile and reference it in an SD-WAN policy rule for specific applications.

(You must also specify which interfaces are available for the firewall to select for error correction by indicating in an SD-WAN Interface Profile that interfaces are **Eligible for Error Correction Profile interface selection**.)

	Error Correction Profile Settings
Name	Add a descriptive name for the Error Correction Profile using a maximum of 31 alphanumeric characters.
Shared	Select to make the Error Correction Profile available to all device groups on Panorama and to every virtual system on a multi-vsys hub or branch to which you push the configuration. Panorama can access an Error Correction Profile that is Shared in the firewall configuration validation and successfully commit and push the configuration to branches and hubs. The commit fails if Panorama cannot reference an Error Correction Profile.
Disable override	Select to prevent administrators from overriding the settings of this Error Correction Profile in device groups that inherit the profile. (**Disable override** is unavailable if **Shared** is selected.)
Activation Threshold (Packet Loss %)	When packet loss exceeds this percentage, FEC or packet duplication is activated for the configured applications in the SD-WAN policy rule where the Error Correction Profile is applied. Range is 1 to 99; default is 2.
Forward Error Correction / Packet Duplication	Select whether to employ forward error correction (FEC) or packet duplication. Packet duplication requires even more resources than FEC.

	Error Correction Profile Settings
Packet Loss Correction Ratio	(Forward Error Correction only) Ratio of parity bits to data packets. The higher the ratio of parity bits to data packets that the encoder sends to the decoder, the higher the probability that the decoder can repair packet loss. However a higher ratio requires more redundancy and therefore more bandwidth overhead, which is a trade-off for achieving error correction. Select one of the predefined ratios: • **10% (20:2)** (Default) • **20% (20:4)** • **30% (20:6)** • **40% (20:8)** • **50% (20:10)** The parity ratio applies to the encoding firewall's outgoing traffic. For example, if the hub parity ratio is 50% and the branch parity ratio is 20%, the hub will receive a ratio of 20% and the branch will receive a ratio of 50%.
Recovery Duration (ms)	Maximum number of milliseconds that the receiving firewall (decoder) can spend performing packet recovery on lost data packets using the parity packets it received; range is 1 to 5,000; default is 1,000. The firewall immediately sends data packets it receives to the destination. During the recovery duration for a block of data, the firewall performs packet recovery for any lost data packets. When the recovery duration expires, the associated parity bits for that block are discarded. The encoder sends the Recovery Duration value to the decoder; the Recovery Duration setting on the decoder has no impact.

Objects > Schedules

By default, Security policy rules are always in effect (all dates and times). To limit a Security policy rule to specific times, you can define schedules, and then apply them to the appropriate policies. For each schedule, you can specify a fixed date and time range or a recurring daily or weekly schedule. To apply schedules to security policies, refer to Policies > Security.

When a Security policy rule is invoked by a defined schedule, only new sessions are affected by the applied Security policy rule. Existing sessions are not affected by the scheduled policy.

Schedule Settings	Description
Name	Enter a schedule name (up to 31 characters). This name appears in the schedule list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared (Panorama only)	Select this option if you want the schedule to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the schedule will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the schedule will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this schedule in device groups that inherit the schedule. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the schedule.
Recurrence	Select the type of schedule (**Daily**, **Weekly**, or **Non-Recurring**).
Daily	Click **Add** and specify a **Start Time** and **End Time** in 24-hour format (HH:MM).
Weekly	Click **Add**, select a **Day of Week**, and specify the **Start Time** and **End Time** in 24-hour format (HH:MM).
Non-recurring	Click **Add** and specify a **Start Date**, **Start Time**, **End Date**, and **End Time**.

Network

The following topics describe the firewall network settings.

- Network > Virtual Wires
- Network > Interfaces
- Network > Virtual Routers
- Network > Zones
- Network > VLANs
- Network > IPSec Tunnels
- Network > GRE Tunnels
- Network > DHCP
- Network > DNS Proxy
- Network > QoS
- Network > LLDP
- Network > Network Profiles

Network > Interfaces

Firewall interfaces (ports) enable a firewall to connect with other network devices and with other interfaces within the firewall. The following topics describe the interface types and how to configure them:

What are you looking for?	See
What are firewall interfaces?	Firewall Interfaces Overview
I am new to firewall interfaces; what are the components of a firewall interface?	Common Building Blocks for Firewall Interfaces Common Building Blocks for PA-7000 Series Firewall Interfaces
I already understand firewall interfaces; how can I find information on configuring a specific interface type?	**Physical Interfaces (Ethernet)** Tap Interface HA Interface Virtual Wire Interface Virtual Wire Subinterface PA-7000 Series Layer 2 Interface PA-7000 Series Layer 2 Subinterface PA-7000 Series Layer 3 Interface Layer 3 Interface Layer 3 Subinterface Log Card Interface Log Card Subinterface Decrypt Mirror Interface Aggregate Ethernet (AE) Interface Group Aggregate Ethernet (AE) Interface **Logical Interfaces** Network > Interfaces > VLAN Network > Interfaces > Loopback Network > Interfaces > Tunnel Network > Interfaces > SD-WAN
Looking for more?	Networking

Firewall Interfaces Overview

The interface configurations of firewall data ports enable traffic to enter and exit the firewall. A Palo Alto Networks® firewall can operate in multiple deployments simultaneously because you can Configure Interfaces to support different deployments. For example, you can configure the Ethernet interfaces on a firewall for virtual wire, Layer 2, Layer 3, and tap mode. The interfaces that the firewall supports are:

- **Physical Interfaces**—The firewall supports two types of media—copper and fiber optic—that can send and receive traffic at different transmission rates. You can configure Ethernet interfaces as the following types: tap, high availability (HA), log card (interface and subinterface), decrypt mirror, virtual wire (interface and subinterface), Layer 2 (interface and subinterface), Layer 3 (interface and subinterface), and aggregate Ethernet. The available interface types and transmission speeds vary by hardware model.
- **Logical Interfaces**—These include virtual local area network (VLAN) interfaces, loopback interfaces, tunnel interfaces, and SD-WAN interfaces. You must set up the physical interface before defining a VLAN, SD-WAN, or tunnel interface.

Common Building Blocks for Firewall Interfaces

Select **Network** > **Interfaces** to display and configure the components that are common to most interface types.

For a description of components that are unique or different when you configure interfaces on a PA-7000 Series firewall, or when you use Panorama™ to configure interfaces on any firewall, see Common Building Blocks for PA-7000 Series Firewall Interfaces*.*

Firewall Interface Building Blocks	Description
Interface (Interface Name)	The interface name is predefined and you cannot change it. However, you can append a numeric suffix for subinterfaces, aggregate interfaces, VLAN interfaces, loopback interfaces, tunnel interfaces, and SD-WAN interfaces.
Interface Type	For Ethernet interfaces (**Network** > **Interfaces** > **Ethernet**), you can select the interface type: • **Tap** • **HA** • **Decrypt Mirror** (Supported on all firewalls except on the VM-Series NSX, Citrix SDX, AWS, and Azure.) • **Virtual Wire** • **Layer 2** • **Layer 3** • **Log Card** (PA-7000 Series firewall only) • **Aggregate Ethernet**
Management Profile	Select a **Management Profile** (**Network** > **Interfaces** > **<if-config** > **Advanced** > **Other Info**) that defines the protocols (such as SSH, Telnet, and HTTP) you can use to manage the firewall over this interface.
Link State	For Ethernet interfaces, Link State indicates whether the interface is currently accessible and can receive traffic over the network: • **Green**—Configured and up • **Red**—Configured but down or disabled • **Gray**—Not configured Hover over the link state to display a tool tip that indicates the link speed and duplex settings for that interface.

Firewall Interface Building Blocks	Description
IP Address	(Optional) Configure the IPv4 or IPv6 address of the Ethernet, VLAN, loopback, or tunnel interface. For an IPv4 address, you can also select the addressing mode (**Type**) for the interface: **Static**, **DHCP Client**, or **PPPoE**.
Virtual Router	Assign a virtual router to the interface or click **Virtual Router** to define a new one (see Network > Virtual Routers). Select **None** to remove the current virtual router assignment from the interface.
Tag (Subinterface only)	Enter the VLAN tag (1-4,094) for the subinterface.
VLAN	Select **Network** > **Interfaces** > **VLAN** and modify an existing **VLAN** or **Add** a new one (see Network > VLANs). Select **None** to remove the current VLAN assignment from the interface. To enable switching between Layer 2 interfaces, or to enable routing through a VLAN interface, you must configure a VLAN object.
Virtual System	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click **Virtual System** to define a new vsys.
Security Zone	Select a **Security Zone** (**Network** > **Interfaces** > **<if-config** > **Config**) for the interface, or select **Zone** to define a new one. Select **None** to remove the current zone assignment from the interface.
Features	For Ethernet interfaces, this column indicates whether the following features are enabled: DHCP Client DNS Proxy GlobalProtect™ gateway enabled Link Aggregation Control Protocol (LACP) Link Layer Discovery Protocol (LLDP) NDP Monitor NetFlow profile Quality of Service (QoS) profile SD-WAN
Comment	A description of the interface function or purpose.

Common Building Blocks for PA-7000 Series Firewall Interfaces

The following table describes the components of the **Network** > **Interfaces** > **Ethernet** page that are unique or different when you configure interfaces on a PA-7000 Series firewall, or when you use Panorama to

configure interfaces on any firewall. Click **Add Interface** to create a new interface or select an existing interface (ethernet1/1, for example) to edit it.

On PA-7000 Series firewalls, you must configure a Log Card Interface on one data port.

PA-7000 Series Firewall Interface Building Blocks	Description
Slot	Select the slot number (1-12) of the interface. Only PA-7000 Series firewalls have multiple slots. If you use Panorama to configure an interface for any other firewall model, select **Slot 1**.
Interface (Interface Name)	Select the name of an interface that is associated with the selected **Slot**.

Tap Interface

- Network > Interfaces > Ethernet

You can use a tap interface to monitor traffic on a port.

To configure a tap interface, click the name of an Interface (ethernet1/1, for example) that is not configured and specify the following information.

Tap Interface Settings	Configured In	Description
Interface Name	**Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select **Tap**.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the interface.
Virtual System	**Ethernet Interface** > **Config**	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system for the interface or click **Virtual System** to define a new vsys.
Security Zone		Select a security zone for the interface or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the interface.
Link Speed	**Ethernet Interface** > **Advanced**	Select the interface speed in Mbps (**10**, **100**, or **1000**), or select **auto** to have the firewall automatically determine the speed.

Tap Interface Settings	Configured In	Description
Link Duplex		Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State		Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).

HA Interface

- Network > Interfaces > Ethernet

Each high availability (HA) interface has a specific function: one interface is for configuration synchronization and heartbeats, and the other interface is for state synchronization. If active/active high availability is enabled, the firewall can use a third HA interface to forward packets.

Some Palo Alto Networks firewalls include dedicated physical ports for use in HA deployments (one for the control link and one for the data link). For firewalls that do not include dedicated ports, you must specify the data ports that will be used for HA. For additional information on HA, refer to "Device > Virtual Systems".

To configure an HA interface, click the name of an Interface (ethernet1/1, for example) that is not configured and specify the following information.

HA Interface Settings	Description
Interface Name	The interface name is predefined and you cannot change it.
Comment	Enter an optional description for the interface.
Interface Type	Select **HA**.
Link Speed	Select the interface speed in Mbps (**10**, **100**, or **1000**), or select **auto** to have the firewall automatically determine the speed.
Link Duplex	Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State	Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).

Virtual Wire Interface

- Network > Interfaces > Ethernet

A virtual wire logically binds two Ethernet interfaces together, allowing for all traffic to pass between the interfaces, or just traffic with selected VLAN tags (no other switching or routing services are available). You can create virtual wire subinterfaces to classify traffic according to an IP address, IP range, or subnet. A virtual wire requires no changes to adjacent network devices. A virtual wire can bind two Ethernet

interfaces of the same medium (both copper or both fiber optic), or bind a copper interface to a fiber optic interface.

To set up a virtual wire, decide which two interfaces to bind (**Network** > **Interfaces** > **Ethernet**) and configure their settings as described in the following table.

If you are using an existing interface for the virtual wire, first remove the interface from any associated security zone.

Virtual Wire Interface Setting	Configured In	Description
Interface Name	**Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select **Virtual Wire**.
Virtual Wire	**Ethernet Interface** > **Config**	Select a virtual wire, or click **Virtual Wire** to define a new one (Network > Virtual Wires). Select **None** to remove the current virtual wire assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system for the interface or click **Virtual System** to define a new vsys.
Security Zone		Select a security zone for the interface, or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the interface.
Link Speed	**Ethernet Interface** > **Advanced**	Select a specific interface speed in Mbps or select **auto** to have the firewall automatically determine the speed. Both interfaces in the virtual wire must have the same speed.
Link Duplex		Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**). Both interfaces in the virtual wire must have the same transmission mode.
Link State		Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).
Enable LLDP	**Ethernet Interface** > **Advanced** > **LLDP**	Select to enable Link Layer Discovery Protocol (LLDP) on the interface. LLDP functions at the link layer to discover neighboring devices and their capabilities.
Profile		If LLDP is enabled, select an LLDP profile to assign to the interface or click **LLDP Profile** to create a new profile (see Network > Network Profiles > LLDP Profile). Select **None** to configure the firewall to use global defaults.
Enable in HA Passive State		If LLDP is enabled, select to configure an HA passive firewall to pre-negotiate LLDP with its peer before the firewall becomes active.

Virtual Wire Interface Setting	Configured In	Description
		If LLDP is not enabled, select to configure an HA passive firewall to simply pass LLDP packets through the firewall.

Virtual Wire Subinterface

- Network > Interfaces > Ethernet

Virtual wire (vwire) subinterfaces allow you to separate traffic by VLAN tags or a VLAN tag and IP classifier combination, assign the tagged traffic to a different zone and virtual system, and then enforce security policies for the traffic that matches the defined criteria.

To add a Virtual Wire Interface select the row for that interface, click **Add Subinterface**, and specify the following information.

Virtual Wire Subinterface Settings	Description
Interface Name	The read-only **Interface Name** displays the name of the vwire interface you selected. In the adjacent field, enter a numeric suffix (1-9,999) to identify the subinterface.
Comment	Enter an optional description for the subinterface.
Tag	Enter the VLAN tag (0-4,094) for the subinterface.
Netflow Profile	If you want to export unidirectional IP traffic that traverses an ingress subinterface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Selecting **None** removes the current NetFlow server assignment from the subinterface.
IP Classifier	Click **Add** and enter an IP address, IP range, or subnet to classify the traffic on this vwire subinterface.
Virtual Wire	Select a virtual wire, or click **Virtual Wire** to define a new one (see Network > Virtual Wires). Select **None** to remove the current virtual wire assignment from the subinterface.
Virtual System	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the subinterface or click **Virtual System** to define a new vsys.
Security Zone	Select a security zone for the subinterface, or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the subinterface.

PA-7000 Series Layer 2 Interface

- Network > Interfaces > Ethernet

Select **Network** > **Interfaces** > **Ethernet** to configure a Layer 2 interface. click the name of an Interface (ethernet1/1, for example) that is not configured and specify the following information.

Layer 2 Interface Settings	Configured In	Description
Interface Name	**Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select **Layer2**.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the interface.
VLAN	**Ethernet Interface** > **Config**	To enable switching between Layer 2 interfaces or to enable routing through a VLAN interface, select an existing VLAN or click **VLAN** to define a new VLAN (see Network > VLANs). Select **None** to remove the current VLAN assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system for the interface or click **Virtual System** to define a new vsys.
Security Zone		Select a **Security Zone** for the interface or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the interface.
Link Speed	**Ethernet Interface** > **Advanced**	Select the interface speed in Mbps (**10**, **100**, or **1000**) or select **auto** to have the firewall automatically determine the speed.
Link Duplex		Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State		Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).
Enable LLDP	**Ethernet Interface** > **Advanced** > **LLDP**	Select to enable Link Layer Discovery Protocol (LLDP) on the interface. LLDP functions at the link layer to discover neighboring devices and their capabilities.
Profile		If LLDP is enabled, select an LLDP profile to assign to the interface or click **LLDP Profile** to create a new profile (see Network > Network Profiles > LLDP Profile). Select **None** to configure the firewall to use global defaults.
Enable in HA Passive State		If LLDP is enabled, select to allow an HA passive firewall to pre-negotiate LLDP with its peer before the firewall becomes active.

PA-7000 Series Layer 2 Subinterface

- Network > Interfaces > Ethernet

For each Ethernet port configured as a physical Layer 2 interface, you can define an additional logical Layer 2 interface (subinterface) for each VLAN tag assigned to the traffic that the port receives. To enable switching between Layer 2 subinterfaces, assign the same VLAN object to the subinterfaces.

To configure a PA-7000 Series Layer 2 Interface, select the row of that physical Interface, click **Add Subinterface**, and specify the following information.

Layer 2 Subinterface Settings	Description
Interface Name	The read-only Interface Name displays the name of the physical interface you selected. In the adjacent field, enter a numeric suffix (1-9,999) to identify the subinterface.
Comment	Enter an optional description for the subinterface.
Tag	Enter the VLAN tag (1-4,094) for the subinterface.
Netflow Profile	If you want to export unidirectional IP traffic that traverses an ingress subinterface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the subinterface.
VLAN	To enable switching between Layer 2 interfaces or to enable routing through a VLAN interface, select a VLAN, or click **VLAN** to define a new VLAN (see Network > VLANs). Select **None** to remove the current VLAN assignment from the subinterface.
Virtual System	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the subinterface or click **Virtual System** to define a new vsys.
Security Zone	Select a security zone for the subinterface or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the subinterface.

PA-7000 Series Layer 3 Interface

- Network > Interfaces > Ethernet

To configure a Layer 3 interface, select an interface (ethernet1/1, for example) and specify the following information.

Layer 3 Interface Settings	Configured In	Description
Interface Name	**Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select **Layer3**.

Layer 3 Interface Settings	Configured In	Description
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the interface.
Virtual Router	**Ethernet Interface** > **Config**	Select a virtual router, or click **Virtual Router** to define a new one (see Network > Virtual Routers). Select **None** to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click **Virtual System** to define a new vsys.
Security Zone		Select a security zone for the interface or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the interface.
Link Speed	**Ethernet Interface** > **Advanced**	Select the interface speed in Mbps (**10**, **100**, or **1000**) or select **auto**.
Link Duplex		Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State		Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).
Management Profile	**Ethernet Interface** > **Advanced** > **Other Info**	Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select **None** to remove the current profile assignment from the interface.
MTU		Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576 to 9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an *ICMP fragmentation needed* message to the source indicating the packet is too large.
Adjust TCP MSS		Select to adjust the maximum segment size (MSS) to accommodate bytes for any headers within the interface MTU byte size. The MTU byte size minus the MSS Adjustment Size equals the MSS byte size, which varies by IP protocol: • **IPv4 MSS Adjustment Size**—Range is 40 to 300; default is 40. • **IPv6 MSS Adjustment Size**—Range is 60 to 300; default is 60. Use these settings to address the case where a **tunnel** through the network requires a smaller MSS. If a packet has more bytes than the MSS without fragmentation, this setting enables the adjustment.

Layer 3 Interface Settings	Configured In	Description
		Encapsulation adds length to headers so it is helpful to configure the MSS adjustment size to allow bytes for such things as an MPLS header or tunneled traffic that has a VLAN tag.
Untagged Subinterface		Specifies that all subinterfaces belonging to this Layer 3 interface are untagged. PAN-OS® selects an untagged subinterface as the ingress interface based on the packet destination. If the destination is the IP address of an untagged subinterface, it maps to the subinterface. This also means that packets in the reverse direction must have their source address translated to the IP address of the untagged subinterface. A byproduct of this classification mechanism is that all multicast and broadcast packets are assigned to the base interface, not any subinterfaces. Because Open Shortest Path First (OSPF) uses multicast, the firewall does not support it on untagged subinterfaces.
IP Address MAC Address	**Ethernet Interface** > **Advanced** > **ARP Entries**	To add one or more static Address Resolution Protocol (ARP) entries, click **Add** and enter an IP address and its associated hardware (MAC) address. To delete an entry, select the entry and click **Delete**. Static ARP entries reduce ARP processing and preclude man-in-the-middle attacks for the specified addresses.
IPv6 Address MAC Address	**Ethernet Interface** > **Advanced** > **ND Entries**	To provide neighbor information for Neighbor Discovery Protocol (NDP), click **Add** and enter the IP address and MAC address of the neighbor.
Enable NDP Proxy	**Ethernet Interface** > **Advanced** > **NDP Proxy**	Select to enable the Neighbor Discovery Protocol (NDP) proxy for the interface. The firewall will respond to ND packets requesting MAC addresses for IPv6 addresses in this list. In the ND response, the firewall sends its own MAC address for the interface to indicate it will act as proxy by responding to packets destined for those addresses. It is recommended that you select **Enable NDP Proxy** if you use Network Prefix Translation IPv6 (NPTv6). If **Enable NDP Proxy** is selected, you can filter numerous Address entries by entering a search string and clicking Apply Filter (→).
Address		Click **Add** to enter one or more IPv6 addresses, IP ranges, IPv6 subnets, or address objects for which the firewall will act as the NDP proxy. Ideally, one of these addresses is the same address as that of the source translation in NPTv6. The order of addresses does not matter. If the address is a subnetwork, the firewall will send an ND response for all addresses in the subnet, so we recommend that you also add the IPv6 neighbors of the firewall and then select **Negate** to instruct the firewall not to respond to these IP addresses.

Layer 3 Interface Settings	Configured In	Description
Negate		Select **Negate** for an address to prevent NDP proxy for that address. You can negate a subset of the specified IP address range or IP subnet.
Enable LLDP	**Ethernet Interface** > **Advanced** > **LLDP**	Select to enable Link Layer Discovery Protocol (LLDP) on the interface. LLDP functions at the link layer to discover neighboring devices and their capabilities.
LLDP Profile		If LLDP is enabled, select an LLDP profile to assign to the interface or click **LLDP Profile** to create a new profile (see Network > Network Profiles > LLDP Profile). Select **None** to configure the firewall to use global defaults.
Enable in HA Passive State		If LLDP is enabled, select to allow the firewall as an HA passive firewall to pre-negotiate LLDP with its peer before the firewall becomes active.
Type	**Ethernet Interface** > **IPv4**	Select the method for assigning an IPv4 address type to the interface: • **Static**—You must manually specify the IP address. • **PPPoE**—The firewall will use the interface for Point-to-Point Protocol over Ethernet (PPPoE). • **DHCP Client**—Enables the interface to act as a Dynamic Host Configuration Protocol (DHCP) client and receive a dynamically assigned IP address. *Firewalls that are in a high availability (HA) active/active configuration do not support PPPoE or DHCP Client.* Based on your IP address method selection, the options displayed in the tab will vary.
Settings	**Ethernet Interface** > **Advanced** > **DDNS**	Select **Settings** to make the DDNS fields available to configure.
Enable		Enable DDNS on the interface. You must initially enable DDNS to configure it. (If your DDNS configuration is unfinished, you can save it without enabling it so that you don't lose your partial configuration.)
Update Interval (days)		Enter the interval (in days) between updates that the firewall sends to the DDNS server to update IP addresses mapped to FQDNs (range is 1 to 30; default is 1). *The firewall also updates DDNS upon receiving a new IP address for the interface from the DHCP server.*

Layer 3 Interface Settings	Configured In	Description
Certificate Profile		Create a Certificate Profile to verify the DDNS service. The DDNS service presents the firewall with a certificate signed by the certificate authority (CA).
Hostname		Enter a hostname for the interface, which is registered with the DDNS Server (for example, host123.domain123.com, or host123). The firewall does not validate the hostname except to confirm that the syntax uses valid characters allowed by DNS for a domain name.
Vendor		Select the DDNS vendor (and version) that provides DDNS service to this interface: • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1**  *If you select an older version of a DDNS service that the firewall indicates will be phased out by a certain date, move to the newer version.* The **Name** and **Value** fields that follow the vendor name are vendor-specific. The read-only fields notify you of parameters that the firewall uses to connect to the DDNS service. Configure the other fields, such as a password that the DDNS service provides to you and a timeout that the firewall uses if it doesn't receive a response from the DDNS server.
IPv4 tab - IP		Add the IPv4 addresses configured on the interface and select them. All selected IP addresses are registered with the DDNS provider (Vendor).
IPv6 tab - IPv6		Add the IPv6 addresses configured on the interface and select them. All selected IP addresses are registered with the DDNS provider (Vendor).
Show Runtime Info		Displays the DDNS registration: DDNS provider, resolved FQDN, and the mapped IP address(es) with an asterisk (*) indicating the primary IP address. Each DDNS provider has its own return codes to indicate the status of the hostname update, and a return date, for troubleshooting purposes.
IPv4 address **Type** = **Static**		
IP	**Ethernet Interface** > **IPv4**	Click **Add**, then perform one of the following steps to specify a static IP address and network mask for the interface. • Type the entry in Classless Inter-domain Routing (CIDR) notation: *ip_address/mask* (for example, 192.168.2.0/24).

Layer 3 Interface Settings	Configured In	Description
		• Select an existing address object of type **IP netmask**. • Click **Address** to create an address object of type **IP netmask**. You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your firewall uses determines the maximum number of IP addresses. To delete an IP address, select the address and click **Delete**.
IPv4 address **Type** = **PPPoE**		
Enable	**Ethernet Interface** > **IPv4** > **PPPoE** > **General**	Select to activate the interface for PPPoE termination.
Username		Enter the username for the point-to-point connection.
Password/Confirm Password		Enter and then confirm the password for the username.
Show PPPoE Client Runtime Info		(Optional) Opens a dialog that displays parameters that the firewall negotiated with the Internet service provider (ISP) to establish a connection. The specific information depends on the ISP.
Authentication	**Ethernet Interface** > **IPv4** > **PPPoE** > **Advanced**	Select the authentication protocol for PPPoE communications: **CHAP** (Challenge-Handshake Authentication Protocol), **PAP** (Password Authentication Protocol), or the default **Auto** (the firewall determines the protocol). Select **None** to remove the current protocol assignment from the interface.
Static Address		Perform one of the following steps to specify the IP address that the Internet service provider assigned (no default value): • Type the entry in Classless Inter-Domain Routing (CIDR) notation: *ip_address/mask* (for example, 192.168.2.0/24). • Select an existing address object of type **IP netmask**. • Click **Address** to create an address object of type **IP netmask**. • Select **None** to remove the current address assignment from the interface.
Automatically create default route pointing to peer		Select to automatically create a default route that points to the PPPoE peer when connected.
Default Route Metric		(Optional) For the route between the firewall and Internet service provider, enter a route metric (priority level) to associate with the default route and to use for path selection (range is 1 to 65,535). The priority level increases as the numeric value decreases.

Layer 3 Interface Settings	Configured In	Description
Access Concentrator		(Optional) Enter the name of the access concentrator on the Internet service provider end to which the firewall connects (no default).
Service		(Optional) Enter the service string (no default).
Passive		Select to use passive mode. In passive mode, a PPPoE end point waits for the access concentrator to send the first frame.
IPv4 address **Type** = **DHCP**		
Enable	**Ethernet Interface** > **IPv4**	Select to activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server		Select to automatically create a default route that points to the default gateway that the DHCP server provides.
Send Hostname		Select to have the firewall (as a DHCP client) send the hostname of the interface (Option 12) to the DHCP server. If you Send Hostname, then the hostname of the firewall is the choice in the hostname field by default. You can send that name or enter a custom hostname (64 characters maximum including uppercase and lowercase letters, numbers, periods, hyphens, and underscores.
Default Route Metric		For the route between the firewall and DHCP server, optionally enter a route metric (priority level) to associate with the default route and to use for path selection (range is 1 to 65,535, no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info		Select to display all settings received from the DHCP server, including DHCP lease status, dynamic IP address assignment, subnet mask, gateway, and server settings (DNS, NTP, domain, WINS, NIS, POP3, and SMTP).
Enable IPv6 on the interface	**Ethernet Interface** > **IPv6**	Select to enable IPv6 addressing on this interface.
Interface ID		Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the **Use interface ID as host portion** option when adding an address, the firewall uses the interface ID as the host portion of that address.
Address		Click **Add** and configure the following parameters for each IPv6 address:

Layer 3 Interface Settings	Configured In	Description
		• **Address**—Enter an IPv6 address and prefix length (for example, 2001:400:f00::1/64). You can also select an existing IPv6 address object or click **Address** to create an address object. • **Enable address on interface**—Select to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Select to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select to include routing through the nearest node. • **Send Router Advertisement**—Select to enable router advertisement (RA) for this IP address. (You must also enable the global **Enable Router Advertisement** option on the interface.) For details on RA, see Enable Router Advertisement. The remaining fields apply only if you enable RA. • **Valid Lifetime**—The length of time, in seconds, that the firewall considers the address as valid. The valid lifetime must equal or exceed the **Preferred Lifetime** (default is 2,592,000). • **Preferred Lifetime**—The length of time, in seconds, that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new connections but any existing connections are valid until the **Valid Lifetime** expires (default is 604,800). • **On-link**—Select if systems that have addresses within the prefix are reachable without a router. • **Autonomous**—Select if systems can independently create an IP address by combining the advertised prefix with an interface ID.
Enable Duplication Address Detection	**Ethernet Interface** > **IPv6** > **Address Resolution**	Select to enable duplicate address detection (DAD), then configure the other fields in this section.
DAD Attempts		Specify the number of DAD attempts within the neighbor solicitation interval (**NS Interval**) before the attempt to identify neighbors fails (range is 1 to 10; default is 1).
Reachable Time		Specify the length of time, in seconds, that a neighbor remains reachable after a successful query and response (range is 10 to 36,000; default is 30).
NS Interval (neighbor solicitation interval)		Specify the number of seconds for DAD attempts before failure is indicated (range is 1 to 10; default is 1).
Enable NDP Monitoring		Select to enable Neighbor Discovery Protocol (NDP) monitoring. When enabled, you can select NDP Monitor ( in

Layer 3 Interface Settings	Configured In	Description
		Features column) and view information about a neighbor that the firewall discovered, such as the IPv6 address, the corresponding MAC address, and the User-ID (on a best-case basis).
Enable Router Advertisement	**Ethernet Interface** > **IPv6** > **Router Advertisement**	To provide stateless address auto-configuration (SLAAC) on IPv6 interfaces, select and configure the other fields in this section. IPv6 DNS clients that receive the router advertisement (RA) messages use this information. RA enables the firewall to act as a default gateway for IPv6 hosts that are not statically configured and to provide the host with an IPv6 prefix for address configuration. You can use a separate DHCPv6 server in conjunction with this feature to provide DNS and other settings to clients. This is a global setting for the interface. If you want to set RA options for individual IP addresses, click **Add** in the IP address table and configure the Address. If you set RA options for any IP address, you must select the **Enable Router Advertisement** option for the interface.
Min Interval (sec)		Specify the minimum interval, in seconds, between RAs that the firewall will send (range is 3 to 1,350; default is 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)		Specify the maximum interval, in seconds, between RAs that the firewall will send (range is 4 to 1,800; default is 600). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit		Specify the hop limit to apply to clients for outgoing packets (range is 1 to 255; default is 64). Enter 0 for no hop limit.
Link MTU		Specify the link maximum transmission unit (MTU) to apply to clients. Select **unspecified** for no link MTU (range is 1,280 to 9,192; default is unspecified).
Reachable Time (ms)		Specify the reachable time (in milliseconds) that the client will use to assume a neighbor is reachable after receiving a reachability confirmation message. Select **unspecified** for no reachable time value (range is 0 to 3,600,000; default is unspecified).
Retrans Time (ms)		Specify the retransmission timer that determines how long the client will wait (in milliseconds) before retransmitting neighbor solicitation messages. Select **unspecified** for no retransmission time (range is 0 to 4,294,967,295; default is unspecified).
Router Lifetime (sec)		Specify how long the client will use the firewall as the default gateway (range is 0 to 9,000; default is 1,800). Zero specifies

Layer 3 Interface Settings	Configured In	Description
		that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
Router Preference		If the network segment has multiple IPv6 routers, the client uses this field to select a preferred router. Select whether the RA advertises the firewall router as having a **High**, **Medium** (default), or **Low** priority relative to other routers on the segment.
Managed Configuration		Select to indicate to the client that addresses are available via DHCPv6.
Consistency Check	**Ethernet Interface** > **IPv6** > **Router Advertisement (cont)**	Select if you want the firewall to verify that RAs sent from other routers are advertising consistent information on the link. The firewall logs any inconsistencies in a system log; the type is **ipv6nd**.
Other Configuration		Select to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Include DNS information in Router Advertisement	**Ethernet Interface** > **IPv6** > **DNS Support**	Select to enable the firewall to send DNS information in NDP router advertisement (RA) messages from this IPv6 Ethernet interface. The other DNS Support fields in this table are visible only after you select this option.
Server		**Add** one or more recursive DNS (RDNS) server addresses for the firewall to send in NDP router advertisements from this IPv6 Ethernet interface. RDNS servers send a series of DNS lookup requests to root DNS and authoritative DNS servers to ultimately provide an IP address to the DNS client. You can configure a maximum of eight RDNS servers that the firewall sends—in the order listed from top to bottom—in an NDP router advertisement to the recipient, which then uses those addresses in the same order. Select a server and **Move Up** or **Move Down** to change the order of the servers or **Delete** a server from the list when you no longer need it.
Lifetime		Enter the maximum number of seconds after the IPv6 DNS client receives the router advertisement before the client can use the RDNS servers to resolve domain names (range is Max Interval (sec) to twice Max Interval; default is 1,200).
Suffix		**Add** and configure one or more domain names (suffixes) for the DNS search list (DNSSL). Maximum length is 255 bytes. A DNS search list is a list of domain suffixes that a DNS client router appends (one at a time) to an unqualified domain name before it enters the name into a DNS query, thereby using a fully qualified domain name in the DNS query. For example, if a DNS client tries to submit a DNS query for “quality” without a suffix, the router appends a period and the first DNS suffix

Layer 3 Interface Settings	Configured In	Description
		from the DNS search list to that name and then transmits the DNS query. If the first DNS suffix on the list is “company.com”, the resulting DNS query from the router is for the FQDN “quality.company.com”. If the DNS query fails, the router appends the second DNS suffix from the list to the unqualified name and transmits a new DNS query. The router tries DNS suffixes until a DNS lookup is successful (ignores the remaining suffixes) or until the router has tried all suffixes on the list. Configure the firewall with the suffixes you want to provide to the DNS client router in a Neighbor Discovery DNSSL option; the DNS client receiving the DNSSL option uses the suffixes in its unqualified DNS queries. You can configure up to eight domain names (suffixes) for a DNS search list that the firewall sends—in order from top to bottom—in an NDP router advertisement to the recipient, which uses those addresses in the same order. Select a suffix and **Move Up** or **Move Down** to change the order or **Delete** a suffix when you no longer need it.
Lifetime		Enter the maximum number of seconds after the IPv6 DNS client receives the router advertisement that it can use a domain name (suffix) on the DNS Search List (range is the value of Max Interval (sec) to twice the Max Interval; default is 1,200).

Layer 3 Interface

- **Network** > **Interfaces** > **Ethernet**

Configure an Ethernet Layer 3 interface to which you can route traffic.

Layer 3 Interface Settings	Description
Interface Name	The read-only **Interface Name** field displays the name of the physical interface you selected.
Comment	Enter a user-friendly description of the interface.
Interface Type	Select **Layer3**.
NetFlow Profile	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the NetFlow profile or select **NetFlow Profile** to create a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the interface.
Config Tab	

Layer 3 Interface Settings	Description
Virtual Router	Assign a virtual router to the interface, or click **Virtual Router** to define a new one (see Network > Virtual Routers). Select **None** to remove the current virtual router assignment from the interface.
Virtual System	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or select **Virtual System** to define a new vsys.
Security Zone	Select a security zone for the interface or select **Zone** to define a new zone. Select **None** to remove the current zone assignment from the interface.
IPv4 Tab	
Enable SD-WAN	Select **Enable SD-WAN** to enable SD-WAN functionality for the Ethernet interface.
Enable Bonjour Reflector	(PA-220, PA-800, and PA-3200 series only) When you enable this option, the firewall forwards Bonjour multicast advertisements and queries received on and forwarded to this interface to all other L3 and AE interfaces and subinterfaces where you enable this option. This helps ensure user access and device discoverability in network environments that use segmentation to route traffic for security or administrative purposes. You can enable this option on up to 16 interfaces.
IPv4 Type = Static	
IP	Add and perform one of the following steps to specify a static IP address and network mask for the interface. • Type the entry in Classless Inter-Domain Routing (CIDR) notation: *ip_address/mask* (for example, 192.168.2.0/24). • Select an existing address object of type **IP netmask**. • Create an **Address** object of type **IP netmask**. You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses. **Delete** an IP address when you no longer need it.
SD-WAN Gateway	If you selected **Enable SD-WAN**, enter the IPv4 address of the SD-WAN gateway.
IPv4 Type = PPPoE, General Tab	
Enable	Select **Enable** to activate the interface for Point-to-Point Protocol over Ethernet (PPPoE) termination. The interface is a PPPoE termination point to support connectivity in a Digital Subscriber Line (DSL) environment where there is a DSL modem but no other PPPoE device to terminate the connection.
Username	Enter the username your ISP provided for the point-to-point connection.
Password and Confirm Password	Enter the password and confirm the password.

Layer 3 Interface Settings	Description
Show PPPoE Client Runtime Info	Select to view information about the PPPoE interface.
IPv4 Type = PPPoE, Advanced Tab	
Authentication	Select an authentication method: • **None**—(default) There is no authentication on the PPPoE interface. • **CHAP**—Firewall uses Challenge Handshake Authentication Protocol —RFC-1994—on the PPPoE interface. • **PAP**—Firewall uses Password Authentication Protocol (PAP) on the PPPoE interface. PAP is less secure than CHAP; PAP sends usernames and passwords in plain text. • **auto**—Firewall negotiates the authentication method (CHAP or PAP) with the PPPoE server.
Static Address	Request from the PPPoE server a desired IPv4 address. PPPoE server may assign that address or another address.
automatically create default route pointing to peer	Select this option to automatically create a default route that points to the default gateway that the PPPoE server provides.
Default Route Metric	Enter the default route metric (priority level) for the PPPoE connection (default is 10). A route with a lower number has higher priority during route selection. For example, a route with a metric of 10 is used before a route with a metric of 100.
Access Concentrator	If your ISP provided the name of an Access Concentrator, enter it. Firewall will connect with this Access Concentrator on the IPS end. This is a string value of 0 to 255 characters.
Service	Firewall (PPPoE client) can provide the desired service request to the PPPoE server. It is a string value of 0 to 255 characters.
Passive	Firewall (PPPOE client) waits for the PPPoE server to initiate a connection. If this is not enabled, firewall initiates a connection.
IPv4 Tab, Type = DHCP Client	
Enable	Enable the interface to act as a Dynamic Host Configuration Protocol (DHCP) client and receive a dynamically assigned IP address.  *Firewalls that are in a high availability (HA) active/active configuration don't support DHCP Client.*
Automatically create default route pointing to	Select this option to cause the firewall to create a static route to a default gateway. The default gateway is useful when clients are trying to access many destinations that don't need to have routes maintained in a routing table on the firewall.

Layer 3 Interface Settings	Description
default gateway provided by server	
Send Hostname	Select this option to assign a hostname to the DHCP client interface and send that hostname (Option 12) to a DHCP server, which can register the hostname with the DNS server. The DNS server can then automatically manage hostname-to-dynamic IP address resolutions. External hosts can identify the interface by its hostname. The default value indicates `system-hostname`, which is the firewall hostname that you set in **Device** > **Setup** > **Management** > **General Settings**. Alternatively, enter a hostname for the interface, which can be a maximum of 64 characters, including uppercase and lowercase letters, numbers, period, hyphen, and underscore.
Default Route Metric	Enter a default route metric (priority level) for the route between the firewall and the DHCP server (range is 1 to 65,535; there is no default metric). A route with a lower number has higher priority during route selection. For example, a route with a metric of 10 is used before a route with a metric of 100.
Show DHCP Client Runtime Info	Select this option to see all of the settings the client has inherited from its DHCP server, including DHCP lease status, dynamic IP address assignment, subnet mask, gateway, and server settings (DNS, NTP, domain, WINS, NIS, POP3, and SMTP).
IPv6 Tab	
Enable IPv6 on the interface	Select to enable IPv6 addressing on the interface.
Interface ID	Enter the 64-bit extended unique identifier (**EUI-64**) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the **Use interface ID as host portion** option when adding an address, the firewall uses the interface ID as the host portion of that address.
Address	Add an IPv6 address and prefix length (for example, 2001:400:f00::1/64). Alternatively, select an existing IPv6 address object or create a new IPv6 address object.
Enable address on interface	Select to enable the IPv6 address on the interface.
Use interface ID as host portion	Select to use the **Interface ID** as the host portion of the IPv6 address.
Anycast	Select to include routing through the nearest node.
Send Router Advertisement	Select to enable router advertisement (RA) for this IP address. (You must also enable the global **Enable Router Advertisement** option on the interface.) For details on RA, see Enable Router Advertisement in this table. The following fields apply only if you Enable Router Advertisement:

Layer 3 Interface Settings	Description
	• **Valid Lifetime**—Length of time, in seconds, that the firewall considers the address valid. The valid lifetime must equal or exceed the **Preferred Lifetime**. The default is 2,592,000. • **Preferred Lifetime**—Length of time, in seconds, that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new connections, but any existing connections are valid until the **Valid Lifetime** expires. The default is 604,800. • **On-link**—Select if systems that have addresses within the prefix are reachable without a router. • **Autonomous**—Select if systems can independently create an IP address by combining the advertised prefix with an interface ID.
IPv6 Tab, Address Resolution Tab	
Enable Duplicate Address Detection	Select to enable duplicate address detection (DAD), then configure the DAD Attempts, Reachable Time (sec), and NS Interval.
DAD Attempts	Specify the number of DAD attempts within the neighbor solicitation interval (**NS Interval**) before the attempt to identify neighbors fails (range is 1 to 10; default is 1).
Reachable Time (sec)	Specify the length of time, in seconds, that a neighbor remains reachable after a successful query and response (range is 1 to 36,000; default is 30).
NS Interval (sec)	Specify the number of seconds for DAD attempts before failure is indicated (range is 1 to 10; default is 1).
Enable NDP Monitoring	Select to enable Neighbor Discovery Protocol (NDP) monitoring. When enabled, you can select NDP (in the Features column) to view information about a neighbor the firewall discovered, such as the IPv6 address, the corresponding MAC address, and the User-ID (on a best-case basis).
IPv6 Tab, Router Advertisement Tab	
Enable Router Advertisement	To provide Neighbor Discovery on IPv6 interfaces, select and configure the other fields in this section. IPv6 DNS clients that receive the router advertisement (RA) messages use this information. RA enables the firewall to act as a default gateway for IPv6 hosts that are not statically configured and to provide the host with an IPv6 prefix for address configuration. You can use a separate DHCPv6 server in conjunction with this feature to provide DNS and other settings to clients. This is a global setting for the interface. If you want to set RA options for individual IP addresses, **Add** and configure an IPv6 address in the IP address table. If you set RA options for any IPv6 address, you must **Enable Router Advertisement** for the interface.

Layer 3 Interface Settings	Description
Min Interval (sec)	Specify the minimum interval, in seconds, between RAs that the firewall will send (range is 3 to 1,350; default is 200). The firewall sends RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)	Specify the maximum interval, in seconds, between RAs that the firewall will send (range is 4 to 1,800; default is 600). The firewall sends RAs at random intervals between the minimum and maximum values you configure.
Hop Limit	Specify the hop limit to apply to clients for outgoing packets (range is 1 to 255; default is 64) or select **unspecified**, which maps to a system default.
Link MTU	Specify the link maximum transmission unit (MTU) to apply to clients (range is 1,280 to 1,500) or default to **unspecified**, which maps to a system default.
Reachable Time (ms)	Specify the reachable time (in milliseconds) that the client will use to assume a neighbor is reachable after receiving a reachability confirmation message (range is 0 to 3,600,000) or default to **unspecified**, which maps to a system default.
Retrans Time (ms)	Specify the retransmission timer that determines how long the client will wait (in milliseconds) before retransmitting neighbor solicitation messages (range is 0 to 4,294,967,295) or default to **unspecified**, which maps to a system default.
Router Lifetime (sec)	Specify how long, in seconds, the client will use the firewall as the default gateway (range is 0 to 9,000; default is 1,800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
Router Preference	If the network segment has multiple IPv6 routers, the client uses this field to select a preferred router. Select whether the RA advertises the firewall router as having a **High**, **Medium** (default), or **Low** priority relative to other routers on the segment.
Managed Configuration	Select to indicate to the client that addresses are available via DHCPv6.
Other Configuration	Select to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check	Select if you want the firewall to verify that RAs sent from other routers are advertising consistent information on the link. The firewall logs any inconsistencies in a system log; the type is **ipv6nd**.
DNS Support Tab Available if you **Enable Router Advertisement** on the **Router Advertisement** Tab)	
Include DNS information in Router Advertisement	Select for the firewall to send DNS information in NDP router advertisements from this IPv6 Ethernet interface. The other DNS Support fields (Server, Lifetime, Suffix, and Lifetime) are visible only after you select this option.
Server	**Add** one or more recursive DNS (RDNS) server addresses for the firewall to send in NDP router advertisements from this IPv6 Ethernet interface. RDNS servers

Layer 3 Interface Settings	Description
	send a series of DNS look up requests to root DNS and authoritative DNS servers to ultimately provide an IP address to the DNS client. You can configure a maximum of eight RDNS Servers that the firewall sends—in order listed from top to bottom—in an NDP router advertisement to the recipient, which then uses them in the same order. Select a server and **Move Up** or **Move Down** to change the order of the servers or **Delete** a server from the list when you no longer need it.
Lifetime	Enter the maximum number of seconds after the IPv6 DNS client receives the router advertisement before the client can use an RDNS server to resolve domain names (range is **Max Interval (sec)** to twice **Max Interval (sec)**; default is 1,200).
Suffix	**Add** one or more domain names (suffixes) for the DNS search list (DNSSL). Maximum length is 255 bytes. A DNS search list is a list of domain suffixes that a DNS client router appends (one at a time) to an unqualified domain name before it enters the name into a DNS query, thereby using a fully qualified domain name in the query. For example, if a DNS client tries to submit a DNS query for the name “quality” without a suffix, the router appends a period and the first DNS suffix from the DNS search list to the name and transmits the DNS query. If the first DNS suffix on the list is “company.com”, the resulting query from the router is for the fully qualified domain name “quality.company.com”. If the DNS query fails, the router appends the second DNS suffix from the list to the unqualified name and transmits a new DNS query. The router uses the DNS suffixes until a DNS lookup is successful (ignores the remaining suffixes) or until the router has tried all of suffixes on the list. Configure the firewall with the suffixes that you want to provide to the DNS client router in a Neighbor Discovery DNSSL option; the DNS client receiving the DNSSL option uses the suffixes in its unqualified DNS queries. You can configure a maximum of 8 domain names (suffixes) for a DNS search list option that the firewall sends—in order listed from top to bottom—in an NDP router advertisement to the recipient, which uses them in the same order. Select a suffix and **Move Up** or **Move Down** to change the order or **Delete** a suffix when you no longer need it.
Lifetime	Enter the maximum number of seconds after the IPv6 DNS client receives the router advertisement that it can use a domain name (suffix) on the DNS search list (range is the value of **Max Interval (sec)** to twice **Max Interval (sec)**; default is 1,200).
SD-WAN Tab	
SD-WAN Interface Status	If you selected **Enable SD-WAN** on the **IPv4** tab, the firewall indicates `SD-WAN Interface Status: Enabled`. If you didn’t **Enable SD-WAN**, it indicates `Disabled`.
SD-WAN Interface Profile	Select the SD-WAN Interface Profile to apply to this Ethernet interface or add a new SD-WAN Interface Profile.

Layer 3 Interface Settings	Description
	You must Enable SD-WAN for the interface before you can apply an SD-WAN Interface Profile.
Upstream NAT	If your SD-WAN hub or branch is behind a device that is performing NAT, **Enable** upstream NAT for the hub or branch.
NAT IP Address Type	Select the type of IP address assignment and specify the IP address or FQDN of the public-facing interface on that NAT-performing device, or specify that DDNS derives the address. Thus, Auto VPN can use the address as the tunnel endpoint of the hub or branch. • **Static IP**—Select the **Type** to be **IP Address** or **FQDN** and enter the IPv4 address or FQDN. • **DDNS**—Dynamic DNS (DDNS) derives the IP address of the upstream NAT device.
Advanced Tab	
Link Speed	Select the interface speed in Mbps (**10**, **100**, or **1000**) or select **auto**.
Link Duplex	Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State	Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).
Advanced Tab. Other Info Tab	
Management Profile	Select a Management profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select **None** to remove the current profile assignment from the interface.
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576 to 9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an *ICMP fragmentation needed* message to the source indicating the packet is too large.
Adjust TCP MSS	Select to adjust the maximum segment size (MSS) to accommodate bytes for any headers within the interface MTU byte size. The MTU byte size minus the MSS Adjustment Size equals the MSS byte size, which varies by IP protocol: • **IPv4 MSS Adjustment Size**—Range is 40 to 300; default is 40. • **IPv6 MSS Adjustment Size**—Range is 60 to 300; default is 60. Use these settings to address the case where a **tunnel** through the network requires a smaller MSS. If a packet has more bytes than the MSS without fragmentation, this setting enables the adjustment. Encapsulation adds length to headers so it helps to configure the MSS adjustment size to allow bytes for such things as an MPLS header or tunneled traffic that has a VLAN tag.

Layer 3 Interface Settings	Description
Untagged Subinterface	Select this option if the corresponding subinterfaces for this interface aren't tagged.
Advanced Tab, ARP Entries Tab	
IP Address MAC Address	To add one or more static Address Resolution Protocol (ARP) entries, **Add** an IP address and its associated hardware [media access control (MAC)] address. To delete an entry, select the entry and click **Delete**. Static ARP entries reduce ARP processing.
Advanced Tab, ND Entries Tab	
IPv6 Address MAC Address	To provide neighbor information for Neighbor Discovery Protocol (NDP), **Add** the IPv6 address and MAC address of the neighbor.
Advanced Tab, NDP Proxy Tab	
Enable NDP Proxy	Enable Neighbor Discovery Protocol (NDP) proxy for the interface. The firewall will respond to ND packets requesting MAC addresses for IPv6 addresses in this list. In the ND response, the firewall sends its own MAC address for the interface so that the firewall will receive the packets meant for the addresses in the list. It is recommended that you enable NDP proxy if you are using Network Prefix Translation IPv6 (NPTv6). If you selected **Enable NDP Proxy**, you can filter numerous **Address** entries by entering a filter and clicking Apply Filter (gray arrow).
Address	**Add** one or more IPv6 addresses, IP ranges, IPv6 subnets, or address objects for which the firewall will act as NDP proxy. Ideally, one of these addresses is the same address as that of the source translation in NPTv6. The order of addresses does not matter. If the address is a subnetwork, the firewall will send an ND response for all addresses in the subnet, so we recommend you also add the IPv6 neighbors of the firewall and then click **Negate** to instruct the firewall not to respond to these IP addresses.
Negate	**Negate** an address to prevent NDP proxy for that address. You can negate a subset of the specified IP address range or IP subnet.
Advanced Tab, LLDP Tab	
Enable LLDP	Enable Link Layer Discovery Protocol (LLDP) for the interface. LLDP functions at the link layer to discover neighboring devices and their capabilities by sending and receiving LLDP data units to and from neighbors.
LLDP Profile	Select an LLDP Profile or create a new LLDP Profile. The profile is the way in which you configure the LLDP mode, enable syslog and SNMP notifications, and configure the optional Type-Length-Values (TLVs) you want transmitted to LLDP peers.

Layer 3 Interface Settings	Description
Advanced Tab, DDNS Tab	
Settings	Select **Settings** to make the DDNS fields available to configure.
Enable	Enable DDNS on the interface. You must initially enable DDNS to configure it. (If your DDNS configuration is unfinished, you can save it without enabling it so that you don't lose your partial configuration.)
Update Interval (days)	Enter the interval (in days) between updates that the firewall sends to the DDNS server to update IP addresses mapped to FQDNs (range is 1 to 30; default is 1). *The firewall also updates DDNS upon receiving a new IP address for the interface from the DHCP server.*
Certificate Profile	Create a Certificate Profile to verify the DDNS service. The DDNS service presents the firewall with a certificate signed by the certificate authority (CA).
Hostname	Enter a hostname for the interface, which is registered with the DDNS Server (for example, host123.domain123.com, or host123). The firewall does not validate the hostname except to confirm that the syntax uses valid characters allowed by DNS for a domain name.
Vendor	Select the DDNS vendor (and version) that provides DDNS service to this interface: • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **Free DNS Afraid.org v1** • **No-IP v1** • (PAN-OS 10.0.3 and later 10.0 releases) **Palo Alto Networks DDNS** (applies only to SD-WAN Full Mesh with DDNS) *If you select an older version of a DDNS service that the firewall indicates will be phased out by a certain date, move to the newer version.* The **Name** and **Value** fields that follow the vendor name are vendor-specific. The read-only fields notify you of parameters that the firewall uses to connect to the DDNS service. Configure the other fields, such as a password that the DDNS service provides to you and a timeout that the firewall uses if it doesn't receive a response from the DDNS server.
IPv4 Tab	Add the IPv4 addresses configured on the interface and then select them. You can select only as many IPv4 addresses as the DDNS provider allows. All selected IP addresses are registered with the DDNS provider (Vendor).
IPv6 Tab	Add the IPv6 addresses configured on the interface and then select them. You can select only as many IPv6 addresses as the DDNS provider allows. All selected IP addresses are registered with the DDNS provider (Vendor).

Layer 3 Interface Settings	Description
Show Runtime Info	Displays the DDNS registration: DDNS provider, resolved FQDN, and the mapped IP address(es) with an asterisk (*) indicating the primary IP address. Each DDNS provider has its own return codes to indicate the status of the hostname update, and a return date, for troubleshooting purposes.

Layer 3 Subinterface

- Network > Interfaces > Ethernet

For each Ethernet port configured as a physical Layer 3 interface, you can define additional logical Layer 3 interfaces (subinterfaces).

To configure a PA-7000 Series Layer 3 Interface, select a physical interface, **Add Subinterface**, and specify the following information.

Layer 3 Subinterface Settings	Configured In	Description
Interface Name	**Layer3 Subinterface**	The read-only **Interface Name** field displays the name of the physical interface you selected. In the adjacent field, enter a numeric suffix (1 to 9,999) to identify the subinterface.
Comment		Enter an optional description for the subinterface.
Tag		Enter the VLAN tag (1 to 4,094) for the subinterface.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress subinterface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the subinterface.
Virtual Router	**Layer3 Subinterface** > **Config**	Assign a virtual router to the interface, or click **Virtual Router** to define a new one (see Network > Virtual Routers). Select **None** to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the subinterface or click **Virtual System** to define a new vsys.
Security Zone		Select a security zone for the subinterface, or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the subinterface.
Type	**Layer3 Subinterface** > **IPv4**	Select the method for assigning an IPv4 address type to the subinterface: • **Static**—You must manually specify the IP address.

Layer 3 Subinterface Settings	Configured In	Description
		• **DHCP Client**—Enables the subinterface to act as a Dynamic Host Configuration Protocol (DHCP) client and receive a dynamically assigned IP address. *Firewalls that are in a high availability (HA) active/active configuration don't support DHCP Client.* Based on your IP address method selection, the options displayed in the tab will vary.
Enable Bonjour Reflector	**Layer3 Subinterface > IPv4**	(PA-220, PA-800, and PA-3200 series only) When you enable this option, the firewall forwards Bonjour multicast advertisements and queries received on and forwarded to this interface to all other L3 and AE interfaces and subinterfaces where you enable this option. This helps ensure user access and device discoverability in network environments that use segmentation to route traffic for security or administrative purposes. You can enable this option on up to 16 interfaces.
IP	**Layer3 Subinterface > IPv4, Type = Static**	**Add** and perform one of the following steps to specify a static IP address and network mask for the interface. • Type the entry in Classless Inter-Domain Routing (CIDR) notation: *ip_address/mask* (for example, 192.168.2.0/24). • Select an existing address object of type **IP netmask**. • Create an **Address** object of type **IP netmask**. You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses. **Delete** an IP address when you no longer need it.
Enable	**Layer3 Subinterface > IPv4, Type = DHCP**	Select to activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server		Select to automatically create a default route that points to the default gateway that the DHCP server provides.
Send Hostname		Select to have the firewall (as a DHCP client) send the hostname of the interface (Option 12) to the DHCP server. If you Send Hostname, by default, then the hostname of the firewall is the choice in the hostname field by default. You can send that name or enter a custom hostname (64 characters maximum including uppercase and lowercase letters, numbers, periods, hyphens, and underscores.
Default Route Metric		(Optional) For the route between the firewall and DHCP server, you can enter a route metric (priority level) to associate with the default route and to use for path selection (range is 1 to 65535;

Layer 3 Subinterface Settings	Configured In	Description
		there is no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info		Select **Show DHCP Client Runtime Info** to display all settings received from the DHCP server, including DHCP lease status, dynamic IP address assignment, subnet mask, gateway, and server settings (DNS, NTP, domain, WINS, NIS, POP3, and SMTP).
Enable IPv6 on the interface	**Layer3 Subinterface > IPv6**	Select to enable IPv6 addressing on this interface.
Interface ID		Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the **Use interface ID as host portion** option when adding an address, the firewall uses the interface ID as the host portion of that address.
Address		Click **Add** and configure the following parameters for each IPv6 address: • **Address**—Enter an IPv6 address and prefix length (for example, 2001:400:f00::1/64). You can also select an existing IPv6 address object or click **Address** to create an address object. • **Enable address on interface**—Select to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Select to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select to include routing through the nearest node. • **Send Router Advertisement**—Select to enable router advertisement (RA) for this IP address. (You must also enable the global **Enable Router Advertisement** option on the interface.) For details on RA, see Enable Router Advertisement in this table. The remaining fields apply only if you enable RA. • **Valid Lifetime**—The length of time, in seconds, that the firewall considers the address as valid. The valid lifetime must equal or exceed the **Preferred Lifetime**. The default is 2,592,000. • **Preferred Lifetime**—The length of time, in seconds, that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new connections but any existing connections are valid until the **Valid Lifetime** expires. The default is 604,800.

Layer 3 Subinterface Settings	Configured In	Description
		• **On-link**—Select if systems that have addresses within the prefix are reachable without a router. • **Autonomous**—Select if systems can independently create an IP address by combining the advertised prefix with an interface ID.
Enable Duplication Address Detection	**Layer3 Subinterface** > **IPv6** > **Address Resolution**	Select to enable duplicate address detection (DAD), then configure the other fields in this section.
DAD Attempts		Specify the number of DAD attempts within the neighbor solicitation interval (**NS Interval**) before the attempt to identify neighbors fails (range is 1 to 10; default is 1).
Reachable Time		Specify the length of time, in seconds, that a neighbor remains reachable after a successful query and response (range is 1 to 36,000; default is 30).
NS Interval (neighbor solicitation interval)		Specify the number of seconds for DAD attempts before failure is indicated (range is 1 to 10; default is 1).
Enable NDP Monitoring		Select to enable Neighbor Discovery Protocol (NDP) monitoring. When enabled, you can select NDP (in Features column) to view information about a neighbor the firewall discovered, such as the IPv6 address, the corresponding MAC address, and the User-ID (on a best-case basis).
Enable Router Advertisement	**Layer3 Subinterface** > **IPv6** > **Router Advertisement**	To provide Neighbor Discovery on IPv6 interfaces, select and configure the other fields in this section. IPv6 DNS clients that receive the router advertisement (RA) messages use this information. RA enables the firewall to act as a default gateway for IPv6 hosts that are not statically configured and to provide the host with an IPv6 prefix for address configuration. You can use a separate DHCPv6 server in conjunction with this feature to provide DNS and other settings to clients. This is a global setting for the interface. If you want to set RA options for individual IP addresses, **Add** and configure an Address in the IP address table. If you set RA options for any IP address, you must **Enable Router Advertisement** for the interface.
Min Interval (sec)		Specify the minimum interval, in seconds, between RAs that the firewall will send (range is 3 to 1,350; default is 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)		Specify the maximum interval, in seconds, between RAs that the firewall will send (range is 4 to 1,800; default is 600). The firewall

Layer 3 Subinterface Settings	Configured In	Description
		will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit		Specify the hop limit to apply to clients for outgoing packets (range is 1 to 255; default is 64). Enter 0 for no hop limit.
Link MTU		Specify the link maximum transmission unit (MTU) to apply to clients. Select **unspecified** for no link MTU (range is 1,280 to 9,192; default is unspecified).
Reachable Time (ms)		Specify the reachable time (in milliseconds) that the client will use to assume a neighbor is reachable after receiving a reachability confirmation message. Select **unspecified** for no reachable time value (range is 0 to 3,600,000; default is unspecified).
Retrans Time (ms)		Specify the retransmission timer that determines how long the client will wait (in milliseconds) before retransmitting neighbor solicitation messages. Select **unspecified** for no retransmission time (range is 0 to 4,294,967,295; default is unspecified).
Router Lifetime (sec)		Specify how long, in seconds, the client will use the firewall as the default gateway (range is 0 to 9,000; default is 1,800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
Router Preference		If the network segment has multiple IPv6 routers, the client uses this field to select a preferred router. Select whether the RA advertises the firewall router as having a **High**, **Medium** (default), or **Low** priority relative to other routers on the segment.
Managed Configuration		Select to indicate to the client that addresses are available via DHCPv6.
Other Configuration		Select to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check	**Layer3 Subinterface** > **IPv6** > **Router Advertisement (cont)**	Select if you want the firewall to verify that RAs sent from other routers are advertising consistent information on the link. The firewall logs any inconsistencies in a system log; the type is **ipv6nd**.
Include DNS information in Router Advertisement	**Layer3 Subinterface** > **IPv6** > **DNS Support**	Select for the firewall to send DNS information in NDP router advertisements from this IPv6 Ethernet subinterface. The other DNS Support fields in this table are visible only after you select this option.

Layer 3 Subinterface Settings	Configured In	Description
Server		**Add** one or more recursive DNS (RDNS) server addresses for the firewall to send in NDP router advertisements from this IPv6 Ethernet interface. RDNS servers send a series of DNS look up requests to root DNS and authoritative DNS servers to ultimately provide an IP address to the DNS client. You can configure a maximum of 8 RDNS Servers that the firewall sends—in order listed from top to bottom—in an NDP router advertisement to the recipient, which then uses them in the same order. Select a server and **Move Up** or **Move Down** to change the order of the servers or **Delete** a server from the list when you no longer need it.
Lifetime		Enter maximum number of seconds after the IPv6 DNS client receives the router advertisement before the client can use an RDNS server to resolve domain names (range is Max Interval (sec) to twice Max Interval; default is 1,200).
Suffix	**Layer3 Subinterface** > **IPv6** > **DNS Support (cont)**	**Add** one or more domain names (suffixes) for the DNS search list (DNSSL). Maximum length is 255 bytes. A DNS search list is a list of domain suffixes that a DNS client router appends (one at a time) to an unqualified domain name before it enters the name into a DNS query, thereby using a fully qualified domain name in the query. For example, if a DNS client tries to submit a DNS query for the name “quality” without a suffix, the router appends a period and the first DNS suffix from the DNS search list to the name and transmits the DNS query. If the first DNS suffix on the list is “company.com”, the resulting query from the router is for the fully qualified domain name “quality.company.com”. If the DNS query fails, the router appends the second DNS suffix from the list to the unqualified name and transmits a new DNS query. The router uses the DNS suffixes until a DNS lookup is successful (ignores the remaining suffixes) or until the router has tried all of suffixes on the list. Configure the firewall with the suffixes that you want to provide to the DNS client router in a Neighbor Discovery DNSSL option; the DNS client receiving the DNSSL option uses the suffixes in its unqualified DNS queries. You can configure a maximum of 8 domain names (suffixes) for a DNS search list option that the firewall sends—in order listed from top to bottom— in an NDP router advertisement to the recipient, which uses them in the same order. Select a suffix and **Move Up** or **Move Down** to change the order or **Delete** a suffix when you no longer need it.
Lifetime	**Layer3 Subinterface** > **IPv6** > **DNS**	Enter the maximum number of seconds after the IPv6 DNS client receives the router advertisement that it can use a domain name

Layer 3 Subinterface Settings	Configured In	Description
	Support (cont)	(suffix) on the DNS search list (range is the value of Max Interval (sec) to twice the Max Interval; default is 1,200).
Management Profile	**Layer3 Subinterface** > **Advanced** > **Other Info**	**Management Profile**—Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select **None** to remove the current profile assignment from the interface.
MTU		Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576 to 9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an *ICMP fragmentation needed* message to the source indicating the packet is too large.
Adjust TCP MSS	**Layer3 Subinterface** > **Advanced** > **Other Info**	Select to adjust the maximum segment size (MSS) to accommodate bytes for any headers within the interface MTU byte size. The MTU byte size minus the MSS Adjustment Size equals the MSS byte size, which varies by IP protocol: • **IPv4 MSS Adjustment Size**—Range is 40 to 300; default is 40. • **IPv6 MSS Adjustment Size**—Range is 60 to 300; default is 60. Use these settings to address the case where a **tunnel** through the network requires a smaller MSS. If a packet has more bytes than the MSS without fragmentation, this setting enables the adjustment. Encapsulation adds length to headers so it helps to configure the MSS adjustment size to allow bytes for such things as an MPLS header or tunneled traffic that has a VLAN tag.
IP Address MAC Address	**Layer3 Subinterface** > **Advanced** > **ARP Entries**	To add one or more static Address Resolution Protocol (ARP) entries, **Add** an IP address and its associated hardware [media access control (MAC)] address. To delete an entry, select the entry and click **Delete**. Static ARP entries reduce ARP processing.
IPv6 Address MAC Address	**Layer3 Subinterface** > **Advanced** > **ND Entries**	To provide neighbor information for Neighbor Discovery Protocol (NDP), **Add** the IP address and MAC address of the neighbor.
Enable NDP Proxy	**Layer3 Subinterface** > **Advanced** > **NDP Proxy**	Enable Neighbor Discovery Protocol (NDP) proxy for the interface. The firewall will respond to ND packets requesting MAC addresses for IPv6 addresses in this list. In the ND response, the firewall sends its own MAC address for the interface so that the firewall will receive the packets meant for the addresses in the list. It is recommended that you enable NDP proxy if you are using Network Prefix Translation IPv6 (NPTv6).

Layer 3 Subinterface Settings	Configured In	Description
		If you selected **Enable NDP Proxy**, you can filter numerous **Address** entries by entering a filter and clicking Apply Filter (gray arrow).
Address		**Add** one or more IPv6 addresses, IP ranges, IPv6 subnets, or address objects for which the firewall will act as NDP proxy. Ideally, one of these addresses is the same address as that of the source translation in NPTv6. The order of addresses does not matter. If the address is a subnetwork, the firewall will send an ND response for all addresses in the subnet, so we recommend you also add the IPv6 neighbors of the firewall and then click **Negate** to instruct the firewall not to respond to these IP addresses.
Negate		**Negate** an address to prevent NDP proxy for that address. You can negate a subset of the specified IP address range or IP subnet.
Settings	**Layer3 Subinterface** > **Advanced** > **DDNS**	Select **Settings** to make the DDNS fields available to configure.
Enable		Enable DDNS on the interface. You must initially enable DDNS to configure it. (If your DDNS configuration is unfinished, you can save it without enabling it so that you don't lose your partial configuration.)
Update Interval (days)	**Layer3 Subinterface** > **Advanced** > **DDNS**	Enter the interval (in days) between updates that the firewall sends to the DDNS server to update IP addresses mapped to FQDNs (range is 1 to 30; default is 1). *The firewall also updates DDNS upon receiving a new IP address for the interface from the DHCP server.*
Certificate Profile		Create a Certificate Profile to verify the DDNS service. The DDNS service presents the firewall with a certificate signed by the certificate authority (CA).
Hostname		Enter a hostname for the interface, which is registered with the DDNS Server (for example, host123.domain123.com, or host123). The firewall does not validate the hostname except to confirm that the syntax uses valid characters allowed by DNS for a domain name.
Vendor	**Layer3 Subinterface** > **Advanced** > **DDNS**	Select the DDNS vendor (and version) that provides DDNS service to this interface: • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1**

Layer 3 Subinterface Settings	Configured In	Description
		• **No-IP v1** *If you select an older version of a DDNS service that the firewall indicates will be phased out by a certain date, move to the newer version.* The **Name** and **Value** fields that follow the vendor name are vendor-specific. The read-only fields notify you of parameters that the firewall uses to connect to the DDNS service. Configure the other fields, such as a password that the DDNS service provides to you and a timeout that the firewall uses if it doesn't receive a response from the DDNS server.
IPv4 tab - IP		Add the IPv4 addresses configured on the interface and then select them. You can select only as many IPv4 addresses as the DDNS provider allows. All selected IP addresses are registered with the DDNS provider (Vendor).
IPv6 tab - IPv6		Add the IPv6 addresses configured on the interface and then select them. You can select only as many IPv6 addresses as the DDNS provider allows. All selected IP addresses are registered with the DDNS provider (Vendor).
Show Runtime Info	**Layer3 Subinterface** > **Advanced** > **DDNS**	Displays the DDNS registration: DDNS provider, resolved FQDN, and the mapped IP address(es) with an asterisk (*) indicating the primary IP address. Each DDNS provider has its own return codes to indicate the status of the hostname update, and a return date, for troubleshooting purposes.

Log Card Interface

- Network > Interfaces > Ethernet

If you configure log forwarding on a PA-7000 Series firewall with a Log Processing Card (LPC), you must configure one data port as type **Log Card**. This is because the traffic and logging capabilities of this firewall model exceed the capabilities of the management (MGT) interface. A log card data port performs log forwarding for syslog, email, Simple Network Management Protocol (SNMP), Panorama log forwarding, and WildFire™ file-forwarding.

You can configure only one port on the firewall as type Log Card. If you enable log forwarding but do not configure an interface with the Log Card type, you get an error when you attempt to commit your changes.

To configure a log card interface, select an Interface that is not configured (ethernet1/16, for example) and configure the settings described in the following table.

Log Card Interface Settings	Configured In	Description
Slot	**Ethernet Interface**	Select the slot number (1-12) of the interface.
Interface Name		The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select **Log Card**.
IPv4	**Ethernet Interface** > **Log Card Forwarding**	If your network uses IPv4, define the following: • **IP address**—The IPv4 address of the port. • **Netmask**—The network mask for the IPv4 address of the port. • **Default Gateway**—The IPv4 address of the default gateway for the port.
IPv6		If your network uses IPv6, define the following: • **IP address**—The IPv6 address of the port. • **Default Gateway**—The IPv6 address of the default gateway for the port.
Link Speed	**Ethernet Interface** > **Advanced**	Select the interface speed in Mbps (**10**, **100**, or **1000**) or select **auto** (default) to have the firewall automatically determine the speed based on the connection. For interfaces that have a non-configurable speed, **auto** is the only option.  *The minimum recommended speed for the connection is 1000 (Mbps).*
Link Duplex		Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically based on the connection (**auto**). The default is **auto**.
Link State		Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically based on the connection (**auto**). The default is **auto**.

Log Card Subinterface

- Network > Interfaces > Ethernet

To add a Log Card Interface, select the row for that interface, **Add Subinterface**, and specify the following information.

Log Card Subinterface Settings	Configured In	Description
Interface Name	**LPC Subinterface**	**Interface Name** (read-only) displays the name of the log card interface you selected. In the adjacent field, enter a numeric suffix (1-9,999) to identify the subinterface.
Comment		Enter an optional description for the interface.
Tag		Enter the VLAN **Tag** (0-4,094) for the subinterface.  *Make the tag the same as the subinterface number for ease of use.*
Virtual System	**LPC Subinterface** > **Config**	Select the virtual system (vsys) to which the Log Processing Card (LPC) subinterface is assigned. Alternatively, you can click **Virtual Systems** to add a new vsys. Once an LPC subinterface is assigned to a vsys, that interface is used as the source interface for all services that forward logs (syslog, email, SNMP) from the log card.
IPv4	**Ethernet Interface** > **Log Card Forwarding**	If your network uses IPv4, define the following: • **IP address**—The IPv4 address of the port. • **Netmask**—The network mask for the IPv4 address of the port. • **Default Gateway**—The IPv4 address of the default gateway for the port.
IPv6		If your network uses IPv6, define the following: • **IP address**—The IPv6 address of the port. • **Default Gateway**—The IPv6 address of the default gateway for the port.

Decrypt Mirror Interface

- Network > Interfaces > Ethernet

To use the Decryption Port Mirror feature, you must select the **Decrypt Mirror** interface type. This feature enables creating a copy of decrypted traffic from a firewall and sending it to a traffic collection tool that can receive raw packet captures—such as NetWitness or Solera—for archiving and analysis. Organizations that require comprehensive data capture for forensic and historical purposes or data leak prevention (DLP) functionality require this feature. To enable the feature, you must acquire and install the free license.

 *Decryption port mirroring is not available on the VM-Series for public cloud platforms (AWS, Azure, Google Cloud Platform), VMware NSX, and Citrix SDX.*

To configure a decrypt mirror interface, click the name of an Interface (ethernet1/1, for example) that is not configured and specify the following information.

Decrypt Mirror Interface Settings	Description
Interface Name	The interface name is predefined and you cannot change it.
Comment	Enter an optional description for the interface.
Interface Type	Select **Decrypt Mirror**.
Link Speed	Select the interface speed in Mbps (**10**, **100**, or **1000**), or select **auto** to have the firewall automatically determine the speed.
Link Duplex	Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State	Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).

Aggregate Ethernet (AE) Interface Group

- Network > Interfaces > Ethernet > Add Aggregate Group

An Aggregate Ethernet (AE) interface group uses IEEE 802.1AX link aggregation to combine multiple Ethernet interfaces in to a single virtual interface that connects the firewall to another network device or another firewall. An AE interface group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy; when one interface fails, the remaining interfaces continue to support traffic.

Before configuring an AE interface group, you must configure its interfaces. Among the interfaces assigned to any particular aggregate group, the hardware media can differ (for example, you can mix fiber optic and copper), but the bandwidth (1Gbps, 10Gbps, 40Gbps, or 100Gbps) and interface type (HA3, virtual wire, Layer 2, or Layer 3) must be the same.

The number of AE interface groups you can add depends on the firewall model. The Product Selection tool indicates the `Maximum aggregate interfaces` that each firewall model supports. Each AE interface group can have up to eight interfaces.

On PA-3200 Series, PA-5200 Series, and most PA-7000 Series firewalls, QoS is supported on only the first eight AE interface groups. The exception is the PA-7000 Series firewall with PA-7000-100G-NPC-A and SMC-B, where QoS is supported on only the first 16 AE interface groups.

All Palo Alto Networks firewalls except the VM-Series models support AE interface groups.

You can aggregate the HA3 (packet forwarding) interfaces in a high availability (HA) active/active configuration but only on the following firewall models:

- *PA-220*
- *PA-800 Series*
- *PA-3200 Series*
- *PA-5200 Series*

To configure an AE interface group, **Add Aggregate Group**, configure the settings described in the following table, and then assign interfaces to the group (see Aggregate Ethernet (AE) Interface).

Aggregate Interface Group Settings	Configured In	Description
Interface Name	**Aggregate Ethernet Interface**	The read-only **Interface Name** is set to **ae**. In the adjacent field, enter a numeric suffix to identify the AE interface group. The range of the numeric suffix depends on how many AE groups the firewall model supports. See the `Maximum aggregate interfaces` supported per firewall model in the Product Selection tool.
Comment		(Optional) Enter a description for the interface.
Interface Type		Select the interface type, which controls the remaining configuration requirements and options: • **HA**—Select only if the interface is an HA3 link between two firewalls in an active/active deployment. Optionally, select a **NetFlow Profile** and configure the settings on the **LACP** tab (see Enable LACP). • **Virtual Wire**—(Optional) Select a **NetFlow Profile** and configure the settings on the **Config** and **Advanced** tabs as described in Virtual Wire Settings. • **Layer 2**—(Optional) Select a **NetFlow Profile**; configure the settings on the **Config** and **Advanced** tabs as described in Layer 2 Interface Settings; and, optionally, configure the **LACP** tab (see Enable LACP). • **Layer 3**—(Optional) Select a **NetFlow Profile**; configure the settings on the **Config** tab, the **IPv4** or **IPv6** tab, and the **Advanced** tab as described in Layer 3 Interface Settings; and, optionally, configure the **LACP** tab (see Enable LACP).
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or **NetFlow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the AE interface group.
Enable LACP	**Aggregate Ethernet Interface > LACP**	Select if you want to enable Link Aggregation Control Protocol (LACP) for the AE interface group. LACP is disabled by default. If you enable LACP, interface failure detection is automatic at the physical and data link layers regardless of whether the firewall and its LACP peer are directly connected. (Without LACP, interface failure detection is automatic only at the physical layer between directly connected peers.) LACP also enables automatic failover to standby interfaces if you configure hot spares (see Max Ports).
Mode		Select the LACP mode of the firewall. Between any two LACP peers, we recommend that you configure one as active and the other as passive. LACP cannot function if both peers are passive. • **Passive** (default)—The firewall passively responds to LACP status queries from peer devices. • **Active**—The firewall actively queries the LACP status (available or unresponsive) of peer devices.

Aggregate Interface Group Settings	Configured In	Description
Transmission Rate		Select the rate at which the firewall exchanges queries and responses with peer devices: • **Fast**—Every second • **Slow** (default)—Every 30 seconds
Fast Failover		Select if, when an interface goes down, you want the firewall to fail over to an operational interface within one second. Otherwise, failover occurs at the standard IEEE 802.1AX-defined speed (at least three seconds).
System Priority	**Aggregate Ethernet Interface** > **LACP (cont)**	The number that determines whether the firewall or its peer overrides the other with respect to port priorities (see **Max Ports** below). *The lower the number, the higher the priority (range is 1 to 65,535; default is 32,768).*
Max Ports		The number of interfaces (1 to 8) that can be active at any given time in an LACP aggregate group. This value cannot exceed the number of interfaces you assign to the group. If the number of assigned interfaces exceeds the number of active interfaces, the firewall uses the LACP port priorities of the interfaces to determine which are in standby mode. You set the LACP port priorities when configuring individual interfaces for the group (see Aggregate Ethernet (AE) Interface).
Enable in HA Passive State		For firewalls deployed in an HA active/passive configuration, select to allow the passive firewall to pre-negotiate LACP with its active peer before a failover occurs. Pre-negotiation speeds up failover because the passive firewall does not have to negotiate LACP before becoming active.
Same System MAC Address for Active-Passive HA	**Aggregate Ethernet Interface** > **LACP (cont)**	This applies only to firewalls deployed in an HA active/passive configuration; firewalls in an active/active configuration require unique MAC addresses. HA firewall peers have the same system priority value. However, in an active/passive deployment, the system ID for each can be the same or different depending on whether you assign the same MAC address. *When the LACP peers (also in HA mode) are virtualized (appearing to the network as a single device), using the same system MAC address for the firewalls minimizes latency during failover. When the LACP peers are not virtualized, using the unique MAC address of each firewall minimizes failover latency.*

Aggregate Interface Group Settings	Configured In	Description
		LACP uses the MAC address to derive a system ID for each LACP peer. If the firewall pair and peer pair have identical system priority values, LACP uses the system ID values to determine which overrides the other with respect to port priorities. If both firewalls have the same MAC address, both will have the same system ID, which will be higher or lower than the system ID of the LACP peers. If the HA firewalls have unique MAC addresses, it is possible for one to have a higher system ID than the LACP peers while the other has a lower system ID. In the latter case, when failover occurs on the firewalls, port prioritization switches between the LACP peers and the firewall that becomes active.
MAC Address	**Aggregate Ethernet Interface** > **LACP (cont)**	If you **Use Same System MAC Address**, select a system-generated MAC address or enter your own MAC address for both firewalls in the active/passive HA pair. You must verify that the address is globally unique.

Aggregate Ethernet (AE) Interface

- Network > Interfaces > Ethernet

To configure an Aggregate Ethernet (AE) Interface, first configure an Aggregate Ethernet (AE) Interface Group and click the name of the interface you will assign to that group. Among the interfaces that you assign to any particular group, the hardware media can differ (for example, you can mix fiber optic and copper), but the bandwidth and interface type (such as Layer 3) must be the same. Furthermore, the interface type must be the same as that defined for the AE interface group, though you will change the type to **Aggregate Ethernet** when you configure each interface. Specify the following information for each interface that you assign to the group.

If you enabled Link Aggregation Control Protocol (LACP) for the AE interface group, select the same Link Speed and Link Duplex for every interface in that group. For non-matching values, the commit operation displays a warning and PAN-OS defaults to the higher speed and full duplex.

Aggregate Interface Settings	Configured In	Description
Interface Name	**Aggregate Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment		(Optional) Enter a description for the interface.
Interface Type		Select **Aggregate Ethernet**.
Aggregate Group		Assign the interface to an aggregate group.

Aggregate Interface Settings	Configured In	Description
Link Speed		Select the interface speed in Mbps (**10**, **100**, or **1000**), or select **auto** to have the firewall automatically determine the speed.
Link Duplex		Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State		Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).
LACP Port Priority		The firewall only uses this field if you enabled Link Aggregation Control Protocol (LACP) for the aggregate group. If the number of interfaces you assign to the group exceeds the number of active interfaces (the Max Ports field), the firewall uses the LACP port priorities of the interfaces to determine which are in standby mode. The lower the numeric value, the higher the priority (range is 1-65,535; default is 32,768).
Virtual Router	**Aggregate Ethernet Interface** > **Config**	Select the virtual router to which you assign the Aggregate Ethernet interface.
Security Zone		Select the security zone to which you assign the Aggregate Ethernet interface.
Enable Bonjour Reflector	**Aggregate Ethernet Interface** > **IPv4**	(PA-220, PA-800, and PA-3200 series only) When you enable this option, the firewall forwards Bonjour multicast advertisements and queries received on and forwarded to this interface to all other L3 and AE interfaces and subinterfaces where you enable this option. This helps ensure user access and device discoverability in network environments that use segmentation to route traffic for security or administrative purposes. You can enable this option on up to 16 interfaces.
Enable IPv6 on the interface	**Aggregate Ethernet Interface** > **IPv6**	Select to enable IPv6 on this interface.
Interface ID		Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you **Use interface ID as host portion** when adding an address, the firewall uses the interface ID as the host portion of that address.
Address		**Add** an IPv6 address and configure the following parameters: • **Address**—Enter an IPv6 address and prefix length (e.g. 2001:400:f00::1/64). You can also select an existing IPv6 address object or click **Address** to create one. • **Enable address on interface**—Select to enable the IPv6 address on the interface.

Aggregate Interface Settings	Configured In	Description
		• **Use interface ID as host portion**—Select to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select to include routing through the nearest node. • **Send RA**—Select to enable router advertisement (RA) for this IP address. When you select this option, you must also globally **Enable Router Advertisement** on the interface. For details on RA, see Enable Router Advertisement. The remaining fields apply are visible only after you enable RA: • **Valid Lifetime**—The length of time, in seconds, that the firewall considers the address as valid. The valid lifetime must equal or exceed the **Preferred Lifetime**. The default is 2,592,000. • **Preferred Lifetime**—The length of time, in seconds, that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new connections but any existing connections are valid until they exceed the **Valid Lifetime**. The default is 604,800. • **On-link**—Select if systems with IP addresses within the advertised prefix are reachable without a router. • **Autonomous**—Select if systems can independently create an IP address by combining the advertised prefix with an interface ID.
Enable Duplication Address Detection	**Aggregate Ethernet Interface** > **IPv6** > **Address Resolution**	Select to enable duplicate address detection (DAD), which then allows you to specify the number of **DAD Attempts**.
DAD Attempts		Specify the number of DAD attempts within the neighbor solicitation interval (**NS Interval**) before the attempt to identify neighbors fails (range is 1-10; default is 1).
Reachable Time		Specify the length of time, in seconds, that a neighbor remains reachable after a successful query and response (range is 1-36,000; default is 30).
NS Interval (neighbor solicitation interval)		Specify the length of time, in seconds, before a DAD attempt failure is indicated (range is 1-10; default is 1).
Enable NDP Monitoring		Select to enable Neighbor Discovery Protocol monitoring. When enabled, you can select the NDP ( in Features column) and view information such as the IPv6 address of a neighbor the firewall has discovered, the corresponding MAC address and User-ID (on a best-case basis).

Aggregate Interface Settings	Configured In	Description
Enable Router Advertisement	**Aggregated Ethernet Interface** > **IPv6** > **Router Advertisement**	Select to provide Neighbor Discovery on IPv6 interfaces and configure the other fields in this section. IPv6 DNS clients that receive the router advertisement (RA) messages use this information. RA enables the firewall to act as a default gateway for IPv6 hosts that are not statically configured and to provide the host with an IPv6 prefix for address configuration. You can use a separate DHCPv6 server in conjunction with this feature to provide DNS and other settings to clients. This is a global setting for the interface. If you want to set RA options for individual IP addresses, **Add** and configure an Address in the IP address table. If you set RA options for any IP address, you must **Enable Router Advertisement** for the interface.
Min Interval (sec)		Specify the minimum interval, in seconds, between RAs that the firewall will send (range is 3-1,350; default is 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)		Specify the maximum interval, in seconds, between RAs that the firewall will send (range is 4-1,800; default is 600). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit		Specify the hop limit to apply to clients for outgoing packets (range is 1-255; default is 64). Enter **0** for no hop limit.
Link MTU		Specify the link maximum transmission unit (MTU) to apply to clients. Select **unspecified** for no link MTU (range is 1,280-9,192; default is unspecified).
Reachable Time (ms)		Specify the reachable time, in milliseconds, that the client will use to assume a neighbor is reachable after receiving a reachability confirmation message. Select **unspecified** for no reachable time value (range is 0-3,600,000; default is unspecified).
Retrans Time (ms)		Specify the retransmission timer that determines how long the client will wait, in milliseconds, before retransmitting neighbor solicitation messages. Select **unspecified** for no retransmission time (range is 0-4,294,967,295; default is unspecified).
Router Lifetime (sec)		Specify how long, in seconds, the client will use the firewall as the default gateway (range is 0-9,000; default is 1,800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.

Aggregate Interface Settings	Configured In	Description
Router Preference		If the network segment has multiple IPv6 routers, the client uses this field to select a preferred router. Select whether the RA advertises the firewall router as having a **High**, **Medium** (default), or **Low** priority relative to other routers on the segment.
Managed Configuration		Select to indicate to the client that addresses are available via DHCPv6.
Other Configuration		Select to indicate to the client that other address information (such as DNS-related settings) is available via DHCPv6.
Consistency Check	**Aggregated Ethernet Interface** > **IPv6** > **Router Advertisement (cont)**	Select if you want the firewall to verify that RAs sent from other routers are advertising consistent information on the link. The firewall logs any inconsistencies in a system log; the type is **ipv6nd**.
Include DNS information in Router Advertisement	**Aggregated Ethernet Interface** > **IPv6** > **DNS Support**	Select for the firewall to send DNS information in NDP router advertisement (RA) messages from this IPv6 Aggregated Ethernet interface. The other DNS Support fields in this table are visible only after you select this option.
Server		**Add** one or more recursive DNS (RDNS) server addresses for the firewall to send in NDP router advertisements from this IPv6 Aggregated Ethernet interface. RDNS servers send a series of DNS lookup requests to root DNS servers and authoritative DNS servers to ultimately provide an IP address to the DNS client. You can configure a maximum of eight RDNS Servers that the firewall sends—in the order listed from top to bottom—in an NDP router advertisement to the recipient, which then uses those addresses in the same order. Select a server and **Move Up** or **Move Down** to change the order of the servers or **Delete** a server when you no longer need it.
Lifetime		Enter the maximum number of seconds after the IPv6 DNS client receives the router advertisement that it can use the RDNS Servers to resolve domain names (range is the value of Max Interval (sec) to twice the Max Interval; default is 1,200).
Suffix		**Add** and configure one or more domain names (suffixes) for the DNS search list (DNSSL). The maximum suffix length is 255 bytes. A DNS search list is a list of domain suffixes that a DNS client router appends (one at a time) to an unqualified domain name before it enters the name into a DNS query, thereby using a fully qualified domain name in the DNS query. For example, if a DNS client tries to submit a DNS query for the name “quality” without a suffix, the router appends a period and the first DNS suffix from the DNS search list to the name and transmits the DNS query.

Aggregate Interface Settings	Configured In	Description
		If the first DNS suffix on the list is “company.com”, the resulting DNS query from the router is for the fully qualified domain name “quality.company.com”. If the DNS query fails, the router appends the second DNS suffix from the list to the unqualified name and transmits a new DNS query. The router tries DNS suffixes until a DNS lookup is successful (ignores the remaining suffixes) or until the router has tried all of suffixes on the list. Configure the firewall with the suffixes you want to provide to the DNS client router in a Neighbor Discovery DNSSL option; the DNS client receiving the DNSSL option uses the suffixes in its unqualified DNS queries. You can configure a maximum of eight domain names (suffixes) for a DNS search list that the firewall sends—in order listed from top to bottom—in an NDP router advertisement to the recipient, which uses them in the same order. Select a suffix and **Move Up** or **Move Down** to change the order of the suffixes or **Delete** a suffix from the list when you no longer need it.
Lifetime	**Aggregated Ethernet Interface** > **IPv6** > **DNS Support (cont)**	Enter the maximum number of seconds after the IPv6 DNS client receives the router advertisement that it can use a domain name (suffix) on the DNS search list (range is the value of Max Interval (sec) to twice the Max Interval; default is 1,200).

Network > Interfaces > VLAN

A VLAN interface can provide routing into a Layer 3 network (IPv4 and IPv6). You can add one or more Layer 2 Ethernet ports (see PA-7000 Series Layer 2 Interface) to a VLAN interface.

VLAN Interface Settings	Configure In	Description
Interface Name	**VLAN Interface**	The read-only **Interface Name** is set to **vlan**. In the adjacent field, enter a numeric suffix (1 to 9,999) to identify the interface.
Comment		Enter an optional description for the interface.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the interface.
VLAN	**VLAN Interface** > **Config**	Select a VLAN or click **VLAN** to define a new one (see Network > VLANs). Select **None** to remove the current VLAN assignment from the interface.
Virtual Router		Assign a virtual router to the interface, or click **Virtual Router** to define a new one (see Network > Virtual Routers). Select **None** to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click **Virtual System** to define a new vsys.
Security Zone		Select a security zone for the interface, or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the interface.
Management Profile	**VLAN Interface** > **Advanced** > **Other Info**	**Management Profile**—Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select **None** to remove the current profile assignment from the interface.
MTU		Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576 to 9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an *ICMP fragmentation needed* message to the source indicating the packet is too large.
Adjust TCP MSS		Select to adjust the maximum segment size (MSS) to accommodate bytes for any headers within the interface MTU byte size. The MTU byte size minus the MSS Adjustment Size equals the MSS byte size, which varies by IP protocol:

VLAN Interface Settings	Configure In	Description
		• **IPv4 MSS Adjustment Size**—Range is 40 to 300; default is 40. • **IPv6 MSS Adjustment Size**—Range is 60 to 300; default is 60. Use these settings to address the case where a **tunnel** through the network requires a smaller MSS. If a packet has more bytes than the MSS without fragmentation, this setting enables the adjustment. Encapsulation adds length to headers, so it helps to configure the MSS adjustment size to allow bytes for such things as an MPLS header or tunneled traffic that has a VLAN tag.
IP Address MAC Address Interface	**VLAN Interface** > **Advanced** > **ARP Entries**	To add one or more static Address Resolution Protocol (ARP) entries, click **Add** and enter an IP address, enter its associated hardware [media access control (MAC)] address, and select a Layer 3 interface that can access the hardware address. To delete an entry, select the entry and click **Delete**. Static ARP entries reduce ARP processing and preclude man-in-the-middle attacks for the specified addresses.
IPv6 Address MAC Address	**VLAN Interface** > **Advanced** > **ND Entries**	To provide neighbor information for Neighbor Discovery Protocol (NDP), click **Add** and enter the IPv6 address and MAC address of the neighbor.
Enable NDP Proxy	**VLAN Interface** > **Advanced** > **NDP Proxy**	Select to enable Neighbor Discovery Protocol (NDP) Proxy for the interface. The firewall will respond to ND packets requesting MAC addresses for IPv6 addresses in this list. In the ND response, the firewall sends its own MAC address for the interface, and is basically saying, “send me the packets meant for these addresses.” (**Recommended**) Enable NDP Proxy if you are using Network Prefix Translation IPv6 (NPTv6). If you **Enable NDP Proxy**, you can filter numerous **Address** entries: first enter a filter and then apply it (green arrow).
Address		**Add** one or more IPv6 addresses, IP ranges, IPv6 subnets, or address objects for which the firewall will act as NDP Proxy. Ideally, one of these addresses is the same address as that of the source translation in NPTv6. The order of addresses does not matter. If the address is a subnetwork, the firewall will send an ND response for all addresses in the subnet, so we recommend you also add the firewall’s IPv6 neighbors and then click **Negate** to instruct the firewall not to respond to these IP addresses.
Negate		Select **Negate** for an address to prevent NDP proxy for that address. You can negate a subset of the specified IP address range or IP subnet.
Settings	**VLAN Interface** >	Select Settings to make the DDNS fields available to configure.
Enable		Enable DDNS on the interface. You must initially enable DDNS to configure it. (If your DDNS configuration is unfinished, you

VLAN Interface Settings	Configure In	Description
	Advanced > **DDNS**	can save it without enabling it so that you don't lose your partial configuration.)
Update Interval (days)		Enter the interval (in days) between updates that the firewall sends to the DDNS server to update IP addresses mapped to FQDNs (range is 1 to 30; default is 1). *The firewall also updates DDNS upon receiving a new IP address for the interface from the DHCP server.*
Certificate Profile		Select a Certificate Profile that you created (or create a new one) to verify the DDNS service. The DDNS service presents the firewall with a certificate signed by the certificate authority (CA).
Hostname		Enter a hostname for the interface, which is registered with the DDNS Server (for example, host123.domain123.com, or host123). The firewall does not validate the hostname except to confirm that the syntax uses valid characters allowed by DNS for a domain name.
Vendor		Select the DDNS vendor (and version number) that provides DDNS service to this interface: • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** *If you select an older version of a DDNS service that the firewall indicates will be phased out by a certain date, move to the newer version.* The **Name** and **Value** fields that follow the vendor name are vendor-specific. Some fields are read-only to notify you of the parameters that the firewall uses to connect to the DDNS service. Configure the other fields, such as a password that the DDNS service provides to you and a timeout the firewall uses if it doesn't receive a response from the DDNS server.
IPv4 tab - IP		Add the IPv4 addresses configured on the interface and select them. All selected IP addresses are registered with the DDNS provider (Vendor).
IPv6 tab - IPv6	**VLAN Interface** > **Advanced** > **DDNS**(cont)	Add the IPv6 addresses configured on the interface and select them. All selected IP addresses are registered with the DDNS provider (Vendor).
Show Runtime Info		Displays the DDNS registration: DDNS provider, resolved FQDN, and the mapped IP address(es) with an asterisk (*) indicating the primary IP address. Each DDNS provider has its own return codes

VLAN Interface Settings	Configure In	Description
		to indicate the status of the hostname update, and a return date, for troubleshooting purposes.
For an IPv4 address		
Type	**VLAN Interface** > **IPv4**	Select the method for assigning an IPv4 address type to the interface: • **Static**—You must manually specify the IP address. • **DHCP Client**—Enables the interface to act as a Dynamic Host Configuration Protocol (DHCP) client and receive a dynamically assigned IP address.  *Firewalls that are in a high availability (HA) active/ active configuration don't support DHCP Client.* Based on your IP address method selection, the options displayed in the tab will vary.
• IPv4 address **Type** = **Static**		
IP	**VLAN Interface** > **IPv4**	Click **Add**, then perform one of the following steps to specify a static IP address and network mask for the interface. • Type the entry in Classless Inter-Domain Routing (CIDR) notation: *ip_address/mask* (for example, 192.168.2.0/24). • Select an existing address object of type **IP netmask**. • Create an **Address** object of type **IP netmask**. You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses. **Delete** an IP address when you no longer need it.
IPv4 address **Type** = **DHCP**		
Enable	**VLAN Interface** > **IPv4**	Select to activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server		Select to automatically create a default route that points to the default gateway that the DHCP server provides.
Send Hostname		Select to configure the firewall (as a DHCP client) to send the hostname of the interface (Option 12) to the DHCP server. If you Send Hostname, then by default, the hostname of the firewall is the choice in the hostname field. You can send that name or enter a

VLAN Interface Settings	Configure In	Description
		custom hostname (64 characters maximum including uppercase and lowercase letters, numbers, periods, hyphens, and underscores.
Default Route Metric		For the route between the firewall and DHCP server, optionally enter a route metric (priority level) to associate with the default route and to use for path selection (range is 1 to 65,535; there is no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info		Select to display all settings received from the DHCP server, including DHCP lease status, dynamic IP address assignment, subnet mask, gateway, and server settings (DNS, NTP, domain, WINS, NIS, POP3, and SMTP).
For an IPv6 address		
Enable IPv6 on the interface	**VLAN Interface > IPv6**	Select to enable IPv6 addressing on this interface.
Interface ID		Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the **Use interface ID as host portion** option when adding an address, the firewall uses the interface ID as the host portion of that address.
Address	**VLAN Interface > IPv6 (cont)**	Click **Add** and configure the following parameters for each IPv6 address: • **Address**—Enter an IPv6 address and prefix length (e.g. 2001:400:f00::1/64). You can also select an existing IPv6 address object or click **Address** to create an address object. • **Enable address on interface**—Select to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Select to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select to include routing through the nearest node. • **Send RA**—Select to enable router advertisement (RA) for this IP address. When you select this option, you must also globally **Enable Router Advertisement** on the interface. For details on RA, see Enable Router Advertisement. The remaining fields apply only if you enable RA. • **Valid Lifetime**—The length of time, in seconds, that the firewall considers the address as valid. The valid lifetime must equal or exceed the **Preferred Lifetime**. The default is 2,592,000. • **Preferred Lifetime**—The length of time, in seconds, that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new

VLAN Interface Settings	Configure In	Description
		connections but any existing connections are valid until they exceed the **Valid Lifetime**. The default is 604,800. • **On-link**—Select if systems with IP addresses within the advertised prefix are reachable without a router. • **Autonomous**—Select if systems can independently create an IP address by combining the advertised prefix with an interface ID.
Enable Duplication Address Detection	**VLAN Interface** > **IPv6** > **Address Resolution**	Select to enable duplicate address detection (DAD), which allows you to specify the number of **DAD Attempts**.
DAD Attempts		Specify the number of DAD attempts within the neighbor solicitation interval (**NS Interval**) before the attempt to identify neighbors fails (range is 1 to 10; default is 1).
Reachable Time		Specify the length of time, in seconds, that a neighbor remains reachable after a successful query and response (range is 1 to 36,000; default is 30).
NS Interval (neighbor solicitation interval)		Specify the number of seconds for DAD attempts before failure is indicated (range is 1 to 10; default is 1).
Enable NDP Monitoring		Select to enable Neighbor Discovery Protocol monitoring. When enabled, you can select the NDP (in Features column) and view information such as the IPv6 address of a neighbor the firewall has discovered, the corresponding MAC address and User-ID (on a best-case basis).
Enable Router Advertisement	**VLAN Interface** > **IPv6** > **Router Advertisement**	Select to provide Neighbor Discovery on IPv6 interfaces and configure the other fields in this section. IPv6 DNS clients that receive the router advertisement (RA) messages use this information. RA enables the firewall to act as a default gateway for IPv6 hosts that are not statically configured and to provide the host with an IPv6 prefix for address configuration. You can use a separate DHCPv6 server in conjunction with this feature to provide DNS and other settings to clients. This is a global setting for the interface. If you want to set RA options for individual IP addresses, **Add** an Address to the IP address table and configure it. If you set RA options for any IP address, you must **Enable Router Advertisement** for the interface.
Min Interval (sec)		Specify the minimum interval, in seconds, between RAs that the firewall will send (range is 3 to 1,350; default is 200). The firewall

VLAN Interface Settings	Configure In	Description
		will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)		Specify the maximum interval, in seconds, between RAs that the firewall will send (range is 4 to 1,800; default is 600). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit		Specify the hop limit to apply to clients for outgoing packets (range is 1 to 255; default is 64). Enter **0** for no hop limit.
Link MTU		Specify the link maximum transmission unit (MTU) to apply to clients. Select **unspecified** for no link MTU (range is 1,280 to 9,192; default is unspecified).
Reachable Time (ms)		Specify the reachable time, in milliseconds, that the client will use to assume a neighbor is reachable after receiving a reachability confirmation message. Select **unspecified** for no reachable time value (range is 0 to 3,600,000; default is unspecified).
Retrans Time (ms)		Specify the retransmission timer that determines how long the client will wait (in milliseconds) before retransmitting neighbor solicitation messages. Select **unspecified** for no retransmission time (range is 0 to 4,294,967,295; default is unspecified).
Router Lifetime (sec)		Specify how long, in seconds, the client will use the firewall as the default gateway (range is 0 to 9,000; default is 1,800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
Router Preference		If the network segment has multiple IPv6 routers, the client uses this field to select a preferred router. Select whether the RA advertises the firewall router as having a **High**, **Medium** (default), or **Low** priority relative to other routers on the segment.
Managed Configuration		Select to indicate to the client that addresses are available via DHCPv6.
Other Configuration		Select to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check	**VLAN Interface** > **IPv6** > **Router Advertisement (cont)**	Select if you want the firewall to verify that RAs sent from other routers are advertising consistent information on the link. The firewall logs any inconsistencies in a system log; the type is **ipv6nd**.
Include DNS information	**VLAN Interface** >	Select for the firewall to send DNS information in NDP router advertisements from this IPv6 VLAN interface. The other DNS

VLAN Interface Settings	Configure In	Description
in Router Advertisement	**IPv6** > **DNS Support**	Support fields in this table are visible only after you select this option.
Server		**Add** one or more recursive DNS (RDNS) server addresses for the firewall to send in NDP router advertisements from this IPv6 VLAN interface. RDNS servers send a series of DNS lookup requests to root DNS servers and authoritative DNS servers to ultimately provide an IP address to the DNS client. You can configure a maximum of eight RDNS servers that the firewall sends— in the order listed from top to bottom—in an NDP router advertisement to the recipient, which then uses them in the same order. Select a server and **Move Up** or **Move Down** to change the order of the servers or **Delete** a server from the list when you no longer need it.
Lifetime		Enter the maximum number of seconds after the IPv6 DNS client receives the router advertisement that it can use the RDNS servers to resolve domain names (range is the value of Max Interval (sec) to twice the Max Interval; default is 1,200).
Suffix		**Add** and configure one or more domain names (suffixes) for the DNS search list (DNSSL). The maximum suffix length is 255 bytes. A DNS search list is a list of domain suffixes that a DNS client router appends (one at a time) to an unqualified domain name before it enters the name into a DNS query, thereby using a fully qualified domain name in the DNS query. For example, if a DNS client tries to submit a DNS query for the name “quality” without a suffix, the router appends a period and the first DNS suffix from the DNS search list to the name and then transmits the DNS query. If the first DNS suffix on the list is “company.com”, the resulting DNS query from the router is for the fully qualified domain name “quality.company.com”. If the DNS query fails, the router appends the second DNS suffix from the list to the unqualified name and transmits a new DNS query. The router tries DNS suffixes until a DNS lookup is successful (ignores the remaining suffixes) or until the router has tried all of suffixes on the list. Configure the firewall with the suffixes that you want to provide to the DNS client router in a Neighbor Discovery DNSSL option; the DNS client receiving the DNSSL option uses the suffixes in its unqualified DNS queries. You can configure a maximum of eight domain names (suffixes) for a DNS search list that the firewall sends—in order listed from top to bottom—in an NDP router advertisement to the recipient, which uses those addresses in the same order. Select a suffix and **Move Up** or **Move Down** to change the order or **Delete** a suffix from the list when you no longer need it.

VLAN Interface Settings	Configure In	Description
Lifetime		Enter the maximum number of seconds after the IPv6 DNS client receives the router advertisement that it can use a domain name (suffix) on the DNS search list (range is the value of Max Interval (sec) to twice the Max Interval; default is 1,200).

Network > Interfaces > Loopback

Use the following fields to configure a loopback interface:

Loopback Interface Settings	Configure In	Description
Interface Name	**Loopback Interface**	The read-only **Interface Name** is set to **loopback**. In the adjacent field, enter a numeric suffix (1-9999) to identify the interface.
Comment		Enter an optional description for the interface.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the interface.
Virtual Router	**Loopback Interface** > **Config**	Assign a virtual router to the interface, or click **Virtual Router** to define a new one (see Network > Virtual Routers). Select **None** to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click **Virtual System** to define a new vsys.
Security Zone		Select a security zone for the interface, or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the interface.
Management Profile	**Tunnel Interface** > **Advanced** > **Other Info**	**Management Profile**—Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select **None** to remove the current profile assignment from the interface.
MTU		Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an *ICMP fragmentation needed* message to the source indicating the packet is too large.
Adjust TCP MSS		Select to adjust the maximum segment size (MSS) to accommodate bytes for any headers within the interface MTU byte size. The MTU byte size minus the MSS Adjustment Size equals the MSS byte size, which varies by IP protocol: • **IPv4 MSS Adjustment Size**—Range is 40-300; default is 40. • **IPv6 MSS Adjustment Size**—Range is 60-300; default is 60.

Loopback Interface Settings	Configure In	Description
		Use these settings to address the case where a **tunnel** through the network requires a smaller MSS. If a packet has more bytes than the MSS without fragmentation, this setting enables the adjustment. Encapsulation adds length to headers, so it helps to configure the MSS adjustment size to allow bytes for such things as an MPLS header or tunneled traffic that has a VLAN tag.
For an IPv4 address		
IP	**Loopback Interface** > **IPv4**	Click **Add**, then perform one of the following steps to specify a static IP address and network mask for the interface. • Enter an IPv4 address with a subnet mask of /32; for example, 192.168.2.1/32. Only a /32 subnet mask is supported. • Select an existing address object of type **IP netmask**. • Click **Address** to create an address object of type **IP netmask**. You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses. To delete an IP address, select the address and click **Delete**.
For an IPv6 address		
Enable IPv6 on the interface	**Loopback Interface** > **IPv6**	Select to enable IPv6 addressing on this interface.
Interface ID		Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the **Use interface ID as host portion** option when adding an address, the firewall uses the interface ID as the host portion of that address.
Address		Click **Add** and configure the following parameters for each IPv6 address: • **Address**—Enter an IPv6 address and prefix length (e.g. 2001:400:f00::1/64). You can also select an existing IPv6 address object or click **Address** to create an address object. • **Enable address on interface**—Select to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Select to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select to include routing through the nearest node.

Network > Interfaces > Tunnel

Use the following fields to configure a tunnel interface:

Tunnel Interface Settings	Configure In	Description
Interface Name	**Tunnel Interface**	The read-only **Interface Name** is set to **tunnel**. In the adjacent field, enter a numeric suffix (1-9,999) to identify the interface.
Comment		Enter an optional description for the interface.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the interface.
Virtual Router	**Tunnel Interface** > **Config**	Assign a virtual router to the interface, or click **Virtual Router** to define a new one (see Network > Virtual Routers). Select **None** to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click **Virtual System** to define a new vsys.
Security Zone		Select a security zone for the interface, or click **Zone** to define a new zone. Select **None** to remove the current zone assignment from the interface.
Management Profile	**Tunnel Interface** > **Advanced** > **Other Info**	**Management Profile**—Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select **None** to remove the current profile assignment from the interface.
MTU		Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an *ICMP fragmentation needed* message to the source indicating the packet is too large.
For an IPv4 address		
IP	**Tunnel Interface** > **IPv4**	Click **Add**, then perform one of the following steps to specify a static IP address and network mask for the interface. • Type the entry in Classless Inter-Domain Routing (CIDR) notation: ip_address/mask (for example, 192.168.2.0/24). • Select an existing address object of type **IP netmask**. • Click **Address** to create an address object of type **IP netmask**.

Tunnel Interface Settings	Configure In	Description
		You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses. To delete an IP address, select the address and click **Delete**.
For an IPv6 address		
Enable IPv6 on the interface	**Tunnel Interface** > **IPv6**	Select to enable IPv6 addressing on this interface.
Interface ID	**Tunnel Interface** > **IPv6**	Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the **Use interface ID as host portion** option when adding an address, the firewall uses the interface ID as the host portion of that address.
Address		Click **Add** and configure the following parameters for each IPv6 address: • **Address**—Enter an IPv6 address and prefix length (e.g. 2001:400:f00::1/64). You can also select an existing IPv6 address object or click **Address** to create an address object. • **Enable address on interface**—Select to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Select to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select to include routing through the nearest node.

Network > Interfaces > SD-WAN

Create a virtual SD-WAN interface and add one or more physical Ethernet interface members that go to the same destination.

SD-WAN Interface Settings	
Interface Name	The read-only **Interface Name** is set to **sdwan**. In the adjacent field, enter a numeric suffix (1 to 9,999) to identify the virtual SD-WAN interface.
Comment	The best practice is to enter a user-friendly description for the interface, such as **`to internet`** or **`to Western USA hub`**. Your comments will make it easier to identify interfaces rather than trying to decipher auto-generated names in logs and reports.
Netflow Profile	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click **Netflow Profile** to define a new profile (see Device > Server Profiles > NetFlow). Select **None** to remove the current NetFlow server assignment from the interface.
Config Tab	
Virtual Router	Assign a virtual router to the interface, or select **Virtual Router** to define a new one (see Network > Virtual Routers). Select **None** to remove the current virtual router assignment from the interface.
Virtual System	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or select **Virtual System** to define a new vsys.
Security Zone	Select a security zone for the interface, or select **Zone** to define a new zone. Select **None** to remove the current zone assignment from the interface. The virtual SD-WAN interface and all of its interface members must be in the same security zone, thus ensuring the same security policy rules apply to all paths from the branch to the same destination.
Advanced Tab	
Interfaces	Select the Layer 3 Ethernet interfaces (for Direct Internet Access [DIA]) or virtual VPN tunnel interfaces (for hub) that constitute this virtual SD-WAN interface. The firewall virtual router uses this virtual SD-WAN interface to route SD-WAN traffic to a DIA or a hub location. The interfaces can have different tags. If you enter more than one interface, they must all be the same type (either VPN tunnel or DIA).

Network > Zones

The following topics describe network security zones.

What are you looking for?	See:
What is the purpose of a security zone?	Security Zone Overview
What are the fields available to configure security zones?	Building Blocks of Security Zones
Looking for more?	Segment Your Network Using Interfaces and Zones

Security Zone Overview

Security zones are a logical way to group physical and virtual interfaces on the firewall to control and log the traffic that traverses specific interfaces on your network. An interface on the firewall must be assigned to a security zone before the interface can process traffic. A zone can have multiple interfaces of the same type assigned to it (such as tap, layer 2, or layer 3 interfaces), but an interface can belong to only one zone.

Policy rules on the firewall use security zones to identify where the traffic comes from and where it is going. Traffic can flow freely within a zone but traffic cannot flow between different zones until you define a Security policy rule that allows it. To allow or deny inter-zone traffic, Security policy rules must reference a source zone and destination zone (not interfaces) and the zones must be of the same type; that is, a Security policy rule can allow or deny traffic from one Layer 2 zone only to another Layer 2 zone.

Building Blocks of Security Zones

To define a security zone, click **Add** and specify the following information.

Security Zone Settings	Description
Name	Enter a zone name (up to 31 characters). This name appears in the list of zones when defining security policies and configuring interfaces. The name is case-sensitive and must be unique within the virtual router. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Location	This field is present only if the firewall supports multiple virtual systems (vsys) and that capability is enabled. Select the vsys to which this zone applies.
Type	Select a zone type (**Tap**, **Virtual Wire**, **Layer2**, **Layer3**, **External**, or **Tunnel**) to view all the **Interfaces** of that type that have not been assigned to a zone. The Layer 2 and Layer 3 zone types list all Ethernet interfaces and subinterfaces of that type. **Add** the interfaces that you want to assign to the zone.

Security Zone Settings	Description
	The External zone is used to control traffic between multiple virtual systems on a single firewall. It displays only on firewalls that support multiple virtual systems and only if the **Multi Virtual System Capability** is enabled. For information on external zones see,Inter-VSYS Traffic That Remains Within the Firewall. An interface can belong to only one zone in one virtual system.
Interfaces	Add one or more interfaces to this zone.
Zone Protection Profiles	Select a profile that specifies how the firewall responds to attacks from this zone. To create a new profile, see Network > Network Profiles > Zone Protection. The best practice is to defend each zone with Zone Protection profile.
Enable Packet Buffer Protection	Configure Packet Buffer Protection (Device > Setup > Session) globally and apply it to each zone. The firewall applies Packet Buffer Protection to the ingress zone only. Packet Buffer Protection based on buffer utilization percentage is enabled by default. An alternative is to configure Packet Buffer Protection based on latency. It is a best practice to enable Packet Buffer Protection on each zone to protect the firewall buffers.
Log Setting	Select a Log Forwarding profile for forwarding zone protection logs to an external system. If you have a Log Forwarding profile named default, that profile will be automatically selected for this drop-down when defining a new security zone. You can override this default setting at any time by continuing to select a different Log Forwarding profile when setting up a new security zone. To define or add a new Log Forwarding profile (and to name a profile default so that this drop-down is populated automatically), click **New** (refer to Objects > Log Forwarding). *If you are configuring the zone in a Panorama template, the Log Setting drop-down lists only shared Log Forwarding profiles; to specify a non-shared profile, you must type its name.*
Enable User Identification	If you configured User-ID™ to perform IP address-to-username mapping (discovery), the best practice is to **Enable User Identification** to apply the mapping information to traffic in this zone. If you disable this option, firewall logs, reports, and policies will exclude user mapping information for traffic within the zone. By default, if you select this option, the firewall applies user mapping information to the traffic of all subnetworks in the zone. To limit the information to specific subnetworks within the zone, use the **Include List** and **Exclude List**. *Enable User-ID on trusted zones only. If you enable User-ID and client probing on an external untrusted zone (such as the internet), probes could be sent outside your protected network, resulting in an information disclosure of the User-ID agent service account name, domain*

Security Zone Settings	Description
	name, and encrypted password hash, which could allow an attacker to gain unauthorized access to protected resources. *User-ID performs discovery for the zone only if it falls within the network range that User-ID monitors. If the zone is outside that range, the firewall does not apply user mapping information to the zone traffic even if you select Enable User Identification. For details, see* Include or Exclude Subnetworks for User Mapping.
User Identification ACL Include List	By default, if you do not specify subnetworks in this list, the firewall applies the user mapping information it discovers to all the traffic of this zone for use in logs, reports, and policies. To limit the application of user mapping information to specific subnetworks within the zone, then for each subnetwork click **Add** and select an address (or address group) object or type the IP address range (for example, 10.1.1.1/24). The exclusion of all other subnetworks is implicit because the **Include List** is an allow list, so you do not need to add them to the **Exclude List**. Add entries to the **Exclude List** only to exclude user mapping information for a subset of the subnetworks in the **Include List**. For example, if you add 10.0.0.0/8 to the **Include List** and add 10.2.50.0/22 to the **Exclude List**, the firewall includes user mapping information for all the zone subnetworks of 10.0.0.0/8 except 10.2.50.0/22, and excludes information for all zone subnetworks outside of 10.0.0.0/8. *You can only include subnetworks that fall within the network range that User-ID monitors. For details, see* Include or Exclude Subnetworks for User Mapping.
User Identification ACL Exclude List	To exclude user mapping information for a subset of the subnetworks in the **Include List**, **Add** an address (or address group) object or type the IP address range for each subnetwork to exclude. *If you add entries to the Exclude List but not the Include List, the firewall excludes user mapping information for all subnetworks within the zone, not just the subnetworks you added.*

Network > VLANs

The firewall supports VLANs that conform to the IEEE 802.1Q standard. Each Layer 2 interface defined on the firewall can be associated with a VLAN. The same VLAN can be assigned to multiple Layer 2 interfaces but each interface can belong to only one VLAN.

VLAN Settings	Description
Name	Enter a VLAN name (up to 31 characters). This name appears in the list of VLANs when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
VLAN Interface	Select a Network > Interfaces > VLAN to allow traffic to be routed outside the VLAN.
Interfaces	Specify firewall interfaces for the VLAN.
Static MAC Configuration	Specify the interface through which a MAC address is reachable. This will override any learned interface-to-MAC mappings.

Network > Virtual Wires

Select **Network** > **Virtual Wires** to define virtual wires after you have specified two virtual wire interfaces on the firewall (Network > Interfaces).

Virtual Wire Settings	Description
Virtual Wire Name	Enter a virtual wire name (up to **31** characters). This name appears in the list of virtual wires when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Interfaces	Select two Ethernet interfaces from the displayed list for the virtual wire configuration. Interfaces are listed here only if they have the virtual wire interface type and have not been assigned to another virtual wire. For information on virtual wire interfaces, see Virtual Wire Interface.
Tag Allowed	Enter the tag number (0-4094) or range of tag numbers (tag1-tag2) for the traffic allowed on the virtual wire. A tag value of zero (default) indicates untagged traffic. Multiple tags or ranges must be separated by commas. Traffic that has an excluded tag value is dropped. *Tag values are not changed on incoming or outgoing packets.* When utilizing virtual wire subinterfaces, the **Tag Allowed** list will cause all traffic with the listed tags to be classified to the parent virtual wire. Virtual wire subinterfaces must utilize tags that do not exist in the parent's **Tag Allowed** list.
Multicast Firewalling	Select if you want to be able to apply security rules to multicast traffic. If this setting is not enabled, multicast traffic is forwarded across the virtual wire.
Link State Pass Through	Select if you want to bring down the other interface in a virtual wire pair when a down link state is detected. If you do not select or you disable this option, link status is not propagated across the virtual wire.

Network > Virtual Routers

The firewall requires a virtual router to obtain routes to other subnets either using static routes that you manually define, or through participation in Layer 3 routing protocols (dynamic routes). Each Layer 3 interface, loopback interface, and VLAN interface defined on the firewall must be associated with a virtual router. Each interface can belong to only one virtual router.

Defining a virtual router requires general settings and any combination of static routes or dynamic routing protocols, as required by your network. You can also configure other features such as route redistribution and ECMP.

What are you looking for?	See
What are the required elements of a virtual router?	General Settings of a Virtual Router
Configure:	Static Routes Route Redistribution RIP OSPF OSPFv3 BGP IP Multicast ECMP
View information about a virtual router.	More Runtime Stats for a Virtual Router
Looking for more?	Networking

General Settings of a Virtual Router

- Network > Virtual Routers > Router Settings > General

All virtual routers require that you assign Layer 3 interfaces and administrative distance metrics as described in the following table.

Virtual Router General Settings	Description
Name	Specify a name to describe the virtual router (up to **31** characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Interfaces	Select the interfaces that you want to include in the virtual router. Thus, they can be used as outgoing interfaces in the virtual router's routing table. To specify the interface type, refer to Network > Interfaces.

Virtual Router General Settings	Description
	When you add an interface, its connected routes are added automatically.
Administrative Distances	Specify the following administrative distances: • **Static routes**—Range is 10-240; default is 10. • **OSPF Int**—Range is 10-240; default is 30. • **OSPF Ext**—Range is 10-240; default is 110. • **IBGP**—Range is 10-240; default is 200. • **EBGP**—Range is 10-240; default is 20. • **RIP**—Range is 10-240; default is 120.

Static Routes

- Network > Virtual Routers > Static Routes

Optionally add one or more static routes. Click the **IP** or **IPv6** tab to specify the route using an IPv4 or IPv6 address. It is usually necessary to configure default routes (0.0.0.0/0) here. Default routes are applied for destinations that are otherwise not found in the virtual router's routing table.

Static Route Settings	Description
Name	Enter a name to identify the static route (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Destination	Enter an IP address and network mask in Classless Inter-domain Routing (CIDR) notation: *ip_address/mask* (for example, 192.168.2.0/24 for IPv4 or 2001:db8::/32 for IPv6). Alternatively, you can create an address object of type IP Netmask.
Interface	Select the interface to forward packets to the destination, or configure the next hop settings, or both.
Next Hop	Select one of the following: • **IP Address**—Select to enter the IP address of the next hop router, or select or create an address object of type IP Netmask. The address object must have a netmask of /32 for IPv4, or /128 for IPv6. • **Next VR**—Select to select a virtual router in the firewall as the next hop. This allows you to route internally between virtual routers within a single firewall. • **FQDN**—Select to identify the next hop by an FQDN. Then select an address object of type FQDN or create a new address object of type FQDN. • **Discard**—Select if you want to drop traffic that is addressed to this destination. • **None**—Select if there is no next hop for the route.
Admin Distance	Specify the administrative distance for the static route (10-240; default is 10).

Static Route Settings	Description
Metric	Specify a valid metric for the static route (1 - 65535).
Route Table	Select the route table into which the firewall installs the static route: • **Unicast**—Installs the route into the unicast route table. • **Multicast**—Installs the route into the multicast route table. • **Both**—Installs the route into the unicast and multicast route tables. • **No Install**—Does not install the route in the route table (RIB); the firewall retains the static route for future reference until you delete the route.
BFD Profile	To enable Bidirectional Forwarding Detection (BFD) for a static route on a PA-3200 Series, PA-5200 Series, PA-7000 Series, or VM-Series firewall, select one of the following: • **default** (default BFD settings) • a BFD profile that you have created on the firewall • **New BFD Profile** to create a new BFD profile Select **None (Disable BFD)** to disable BFD for the static route. To use BFD on a static route: • Both the firewall and the peer at the opposite end of the static route must support BFD sessions. • The static route **Next Hop** type must be **IP Address** and you must enter a valid IP address. • The **Interface** setting cannot be **None**; you must select an interface (even if you are using a DHCP address).
Path Monitoring	Select to enable path monitoring for the static route.
Failure Condition	Select the condition under which the firewall considers the monitored path down and thus the static route down: • **Any**—If any one of the monitored destinations for the static route is unreachable by ICMP, the firewall removes the static route from the RIB and FIB and adds the dynamic or static route that has the next lowest metric going to the same destination to the FIB. • **All**—If all of the monitored destinations for the static route are unreachable by ICMP, the firewall removes the static route from the RIB and FIB and adds the dynamic or static route that has the next lowest metric going to the same destination to the FIB. Select **All** to avoid the possibility of a single monitored destination signaling a static route failure when that monitored destination is simply offline for maintenance, for example.
Preemptive Hold Time (min)	Enter the number of minutes a downed path monitor must remain in Up state—the path monitor evaluates all of its member monitored destinations and must remain Up before the firewall reinstalls the static route into the RIB. If the timer expires without the link going down or flapping, the link is deemed stable, path monitor can remain Up, and the firewall can add the static route back into the RIB.

Static Route Settings	Description
	If the link goes down or flaps during the hold time, path monitor fails and the timer restarts when the downed monitor returns to Up state. A **Preemptive Hold Time** of zero causes the firewall to reinstall the static route into the RIB immediately upon the path monitor coming up. Range is 0-1,440; default is 2.
Name	Enter a name for the monitored destination (up to 31 characters).
Enable	Select to enable path monitoring of this specific destination for the static route; the firewall sends ICMP pings to this destination.
Source IP	Select the IP address that the firewall will use as the source in the ICMP ping to the monitored destination: • If the interface has multiple IP addresses, select one. • If you select an interface, the firewall uses the first IP address assigned to the interface by default. • If you select **DHCP (Use DHCP Client address)**, the firewall uses the address that DHCP assigned to the interface. To see the DHCP address, select **Network** > **Interfaces** > **Ethernet** and in the row for the Ethernet interface, click on **Dynamic DHCP Client**. The IP Address appears in the Dynamic IP Interface Status window.
Destination IP	Enter a robust, stable IP address or address object for which the firewall will monitor the path. The monitored destination and the static route destination must use the same address family (IPv4 or IPv6)
Ping Interval (sec)	Specify the ICMP ping interval in seconds to determine how frequently the firewall monitors the path (pings the monitored destination; range is 1-60; default is 3).
Ping Count	Specify the number of consecutive ICMP ping packets that do not return from the monitored destination before the firewall considers the link down. Based on the **Any** or **All** failure condition, if path monitoring is in failed state, the firewall removes the static route from the RIB (range is 3-10; default is 5). For example, a Ping Interval of 3 seconds and Ping Count of 5 missed pings (the firewall receives no ping in the last 15 seconds) means path monitoring detects a link failure. If path monitoring is in failed state and the firewall receives a ping after 15 seconds, the link is deemed up; based on the **Any** or **All** failure condition, path monitoring to **Any** or **All** monitored destinations can be deemed up, and the Preemptive Hold Time starts.

Route Redistribution

- Network > Virtual Router > Redistribution Profiles

Redistribution profiles direct the firewall to filter, set priority, and perform actions based on desired network behavior. Route redistribution allows static routes and routes that are acquired by other protocols to be advertised through specified routing protocols.

Redistribution profiles must be applied to routing protocols in order to take effect. Without redistribution rules, each protocol runs separately and does not communicate outside its purview. Redistribution profiles can be added or modified after all routing protocols are configured and the resulting network topology is established.

Apply redistribution profiles to the RIP and OSPF protocols by defining export rules. Apply redistribution profiles to BGP in the **Redistribution Rules** tab. Refer to the following table.

Redistribution Profile Settings	Description
Name	**Add** a **Redistribution Profile** and enter the profile name.
Priority	Enter a priority (range is 1-255) for this profile. Profiles are matched in order (lowest number first).
Redistribute	Choose whether to perform route redistribution based on the settings in this window. • **Redist**—Select to redistribute matching candidate routes. If you select this option, enter a new metric value. A lower metric value means a more preferred route. • **No Redist**—Select to not redistribute matching candidate routes.
General Filter Tab	
Type	Select the route types of the candidate route.
Interface	Select the interfaces to specify the forwarding interfaces of the candidate route.
Destination	To specify the destination of the candidate route, enter the destination IP address or subnet (format x.x.x.x or x.x.x.x/n) and click **Add**. To remove an entry, click remove (⊖).
Next Hop	To specify the gateway of the candidate route, enter the IP address or subnet (format x.x.x.x or x.x.x.x/n) that represents the next hop and click **Add**. To remove an entry, click remove (⊖).
OSPF Filter Tab	
Path Type	Select the route types of the candidate OSPF route.
Area	Specify the area identifier for the candidate OSPF route. Enter the **OSPF area ID** (format x.x.x.x), and click **Add**. To remove an entry, click remove (⊖).
Tag	Specify OSPF tag values. Enter a numeric tag value (1-255), and click Add. To remove an entry, click remove (⊖).
BGP Filter Tab	

Redistribution Profile Settings	Description
Community	Specify a community for BGP routing policy.
Extended Community	Specify an extended community for BGP routing policy.

RIP

- Network > Virtual Routers > RIP

Configuring the Routing Information Protocol (RIP) includes the following general settings:

RIP Settings	Description
Enable	Select to enable RIP.
Reject Default Route	(Recommended) Select if you do not want to learn any default routes through RIP.
BFD	To enable Bidirectional Forwarding Detection (BFD) for RIP globally for the virtual router on a PA-5200 Series, PA-7000 Series, and VM-Series firewall, select one of the following: • **default** (profile with the default BFD settings) • a BFD profile that you have created on the firewall • **New BFD Profile** to create a new BFD profile Select **None (Disable BFD)** to disable BFD for all RIP interfaces on the virtual router; you cannot enable BFD for a single RIP interface.

In addition, RIP settings on the following tabs must be configured:

- **Interfaces**: See RIP Interfaces Tab.
- **Timers**: See RIP Timers Tab.
- **Auth Profiles**: See RIP Auth Profiles Tab.
- **Export Rules**: See RIP Export Rules Tab.

RIP Interfaces Tab

- Network > Virtual Routers > RIP > Interfaces

Use the following fields to configure RIP interfaces:

RIP – Interface Settings	Description
Interface	Select the interface that runs the RIP protocol.
Enable	Select to enable these settings.
Advertise	Select to enable advertisement of a default route to RIP peers with the specified metric value.

RIP – Interface Settings	Description
Metric	Specify a metric value for the router advertisement. This field is visible only if you enable **Advertise**.
Auth Profile	Select the profile.
Mode	Select **normal**, **passive**, or **send-only**.
BFD	To enable BFD for a RIP interface (and thereby override the BFD setting for RIP, as long as BFD is not disabled for RIP at the virtual router level), select one of the following: • **default** (profile with the default BFD settings) • a BFD profile that you created on the firewall • **New BFD Profile** to create a new BFD profile Select **None (Disable BFD)** to disable BFD for the RIP interface.

RIP Timers Tab

- Network > Virtual Router > RIP > Timers

The following table describes the timers that control RIP route updates and expirations.

RIP – Timer Settings	Description
RIP Timing	
Interval Seconds (sec)	Define the length of the timer interval in seconds. This duration is used for the remaining RIP timing fields (range is 1-60).
Update Intervals	Enter the number of intervals between route update announcements (range is 1-3,600).
Expire Intervals	Enter the number of intervals between the time that the route was last updated to its expiration (range is 1-3,600).
Delete Intervals	Enter the number of intervals between the time that the route expires to its deletion (range is 1-3,600).

RIP Auth Profiles Tab

- Network > Virtual Router > RIP > Auth Profiles

By default, the firewall does not authenticate RIP messages between neighbors. To authenticate RIP messages between neighbors, create an authentication profile and apply it to an interface running RIP on a virtual router. The following table describes the settings for the **Auth Profiles** tab.

RIP – Auth Profile Settings	Description
Profile Name	Enter a name for the authentication profile to authenticate RIP messages.

RIP – Auth Profile Settings	Description
Password Type	Select the type of password (simple or MD5). • If you select **Simple**, enter the simple password and then confirm. • If you select **MD5**, enter one or more password entries, including **Key-ID** (0-255), **Key**, and optional **Preferred** status. Click **Add** for each entry, and then click **OK**. To specify the key to be used to authenticate outgoing message, select the **Preferred** option.

RIP Export Rules Tab

- Network > Virtual Router > RIP > Export Rules

RIP export rules allow you to control which routes the virtual router sends to peers.

RIP – Export Rules Settings	Description
Allow Redistribute Default Route	Select to permit the firewall to redistribute its default route to peers.
Redistribution Profile	Click **Add** and select or create a redistribution profile that allows you to modify route redistribution, filter, priority, and action based on the desired network behavior. Refer to Route Redistribution.

OSPF

- Network > Virtual Router > OSPF

Configuring the Open Shortest Path First (OSPF) protocol requires you to configure the following general settings (except BFD, which is optional):

OSPF Settings	Description
Enable	Select to enable the OSPF protocol.
Reject Default Route	(Recommended) Select if you do not want to learn any default routes through OSPF.
Router ID	Specify the router ID associated with the OSPF instance in this virtual router. The OSPF protocol uses the router ID to uniquely identify the OSPF instance.
BFD	To enable Bidirectional Forwarding Detection (BFD) for OSPF globally for the virtual router on a PA-5200 Series, PA-7000 Series, or VM-Series firewall, select one of the following: • **default** (default BFD settings) • a BFD profile that you have created on the firewall • **New BFD Profile** to create a new BFD profile

OSPF Settings	Description
	Select **None (Disable BFD)** to disable BFD for all OSPF interfaces on the virtual router; you cannot enable BFD for a single OSPF interface.

In addition, you must configure OSPF settings on the following tabs:

- **Areas**: See OSPF Areas Tab.
- **Auth Profiles**: See OSPF Auth Profiles Tab.
- **Export Rules**: See OSPF Export Rules Tab.
- **Advanced**: See OSPF Advanced Tab.

OSPF Areas Tab

- Network > Virtual Router > OSPF > Areas

The following fields describe the OSPF area settings:

OSPF – Areas Settings	Description
Areas	
Area ID	Configure the area over which the OSPF parameters can be applied. Enter an identifier for the area in x.x.x.x format. This is the identifier that each neighbor must accept to be part of the same area.
Type	Select one of the following options. • **Normal**—There are no restrictions; the area can carry all types of routes. • **Stub**—There is no outlet from the area. To reach a destination outside of the area, it is necessary to go through the border, which connects to other areas. If you select this option, select **Accept Summary** if you want to accept this type of link state advertisement (LSA) from other areas. Also, specify whether to include a default route LSA in advertisements to the stub area along with the associated metric value (range is 1-255). If the **Accept Summary** option on a stub area Area Border Router (ABR) interface is disabled, the OSPF area will behave as a Totally Stubby Area (TSA) and the ABR will not propagate any summary LSAs. • **NSSA** (Not-So-Stubby Area)—It is possible to leave the area directly, but only by routes other than OSPF routes. If you select this option, select **Accept Summary** if you want to accept this type of LSA. Select **Advertise Default Route** to specify whether to include a default route LSA in advertisements to the stub area along with the associated metric value (1-255). Also, select the route type used to advertise the default LSA. Click **Add** in the **External Ranges** section and enter ranges if you want to enable or suppress advertising external routes that are learned through NSSA to other areas.
Range	Click **Add** to aggregate LSA destination addresses in the area into subnets. Enable or suppress advertising LSAs that match the subnet, and click **OK**. Repeat to add additional ranges.

OSPF – Areas Settings	Description
Interface	**Add** an interface to be included in the area and enter the following information: • **Interface**—Choose the interface. • **Enable**—Cause the OSPF interface settings to take effect. • **Passive**—Select if you do not want the OSPF interface to send or receive OSPF packets. Although OSPF packets are not sent or received if you choose this option, the interface is included in the LSA database. • **Link type**—Choose **Broadcast** if you want all neighbors that are accessible through the interface to be discovered automatically by multicasting OSPF hello messages, such as an Ethernet interface. Choose **p2p** (point-to-point) to automatically discover the neighbor. Choose **p2mp** (point-to-multipoint) when neighbors must be defined manually. Defining neighbors manually is allowed only for p2mp mode. • **Metric**—Enter the OSPF metric for this interface (0-65,535). • **Priority**—Enter the OSPF priority for this interface (0-255). It is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) according to the OSPF protocol. When the value is zero, the router will not be elected as a DR or BDR. • **Auth Profile**—Select a previously-defined authentication profile. • **BFD**—To enable Bidirectional Forwarding Detection (BFD) for an OSPF peer interface (and thereby override the **BFD** setting for OSPF, as long as **BFD** is not disabled for OSPF at the virtual router level), select one of the following: • **default** (default BFD settings) • a BFD profile that you have created on the firewall • **New BFD Profile** to create a new BFD profile • Select **None (Disable BFD)** to disable BFD for the OSPF peer interface. • **Hello Interval (sec)**—Interval, in seconds, at which the OSPF process sends hello packets to its directly connected neighbors (range is 0-3600; default is 10). • **Dead Counts**—Number of times the hello interval can occur for a neighbor without OSPF receiving a hello packet from the neighbor, before OSPF considers that neighbor down. The **Hello Interval** multiplied by the **Dead Counts** equals the value of the dead timer (range is 3-20; default is 4). • **Retransmit Interval (sec)**—Length of time, in seconds, that OSPF waits to receive a link-state advertisement (LSA) from a neighbor before OSPF retransmits the LSA (range is 0-3,600; default is 10). • **Transit Delay (sec)**—Length of time, in seconds, that an LSA is delayed before it is sent out of an interface (range is 0-3,600; default is 1).
Interface (cont)	• **Graceful Restart Hello Delay (sec)**—Applies to an OSPF interface when Active/Passive High Availability is configured. **Graceful Restart Hello Delay** is the length of time during which the firewall sends Grace LSA packets at 1-second intervals. During this time, no hello packets are sent from the restarting firewall. During the restart, the dead timer (which is the **Hello Interval** multiplied by the **Dead Counts**) is also counting down. If the dead timer is too short, the adjacency will go

OSPF – Areas Settings	Description
	down during the graceful restart because of the hello delay. Therefore, it is recommended that the dead timer be at least four times the value of the **Graceful Restart Hello Delay**. For example, a **Hello Interval** of 10 seconds and a **Dead Counts** of 4 yield a dead timer of 40 seconds. If the **Graceful Restart Hello Delay** is set to 10 seconds, that 10-second delay of hello packets is comfortably within the 40-second dead timer, so the adjacency will not time out during a graceful restart (range is 1-10; default is 10).
Virtual Link	Configure the virtual link settings to maintain or enhance backbone area connectivity. The settings must be defined for area boarder routers, and must be defined within the backbone area (0.0.0.0). Click **Add**, enter the following information for each virtual link to be included in the backbone area, and click **OK**. • **Name**—Enter a name for the virtual link. • **Neighbor ID**—Enter the router ID of the router (neighbor) on the other side of the virtual link. • **Transit Area**—Enter the area ID of the transit area that physically contains the virtual link. • **Enable**—Select to enable the virtual link. • **Timing**—It is recommended that you keep the default timing settings. • **Auth Profile**—Select a previously-defined authentication profile.

OSPF Auth Profiles Tab

- Network > Virtual Router > OSPF > Auth Profiles

The following fields describe the OSPF authentication profile settings:

OSPF – Auth Profile Settings	Description
Profile Name	Enter a name for the authentication profile. To authenticate the OSPF messages, first define the authentication profiles and then apply them to interfaces on the **OSPF** tab.
Password Type	Select the type of password (simple or MD5). • If you select **Simple**, enter the password. • If you select **MD5**, enter one or more password entries, including **Key-ID** (0-255), **Key**, and optional **Preferred** status. Click **Add** for each entry, and then click **OK**. To specify the key to be used to authenticate outgoing message, select the **Preferred** option.

OSPF Export Rules Tab

- Network > Virtual Router > OSPF > Export Rules

The following table describes the fields to export OSPF routes:

OSPF – Export Rules Settings	Description
Allow Redistribute Default Route	Select to permit redistribution of default routes through OSPF.
Name	Select the name of a redistribution profile. The value must be an IP subnet or valid redistribution profile name.
New Path Type	Choose the metric type to apply.
New Tag	Specify a tag for the matched route that has a 32-bit value.
Metric	(Optional) Specify the route metric to be associated with the exported route and used for path selection (range is 1-65,535).

OSPF Advanced Tab

- Network > Virtual Router > OSPF > Advanced

The following fields describe RFC 1583 compatibility, OSPF timers, and graceful restart:

OSPF – Advanced Settings	Description
RFC 1583 Compatibility	Select to ensure compatibility with RFC 1583 (OSPF Version 2).
Timers	• **SPF Calculation Delay (sec)**—Allows you to tune the delay time between receiving new topology information and performing an SPF calculation. Lower values enable faster OSPF re-convergence. Routers peering with the firewall should be tuned in a similar manner to optimize convergence times. • **LSA Interval (sec)**—Specifies the minimum time between transmissions of two instances of the same LSA (same router, same type, same LSA ID). This is equivalent to MinLSInterval in RFC 2328. Lower values can be used to reduce re-convergence times when topology changes occur.
Graceful Restart	• **Enable Graceful Restart**—Enabled by default, a firewall enabled for this feature will instruct neighboring routers to continue using a route through the firewall while a transition takes place that renders the firewall temporarily down. • **Enable Helper Mode**—Enabled by default, a firewall enabled for this mode continues to forward to an adjacent device when that device is restarting. • **Enable Strict LSA Checking**—Enabled by default, this feature causes an OSPF helper mode enabled firewall to exit helper mode if a topology change occurs. • **Grace Period (sec)**—Period of time, in seconds, that peer devices should continue to forward to this firewall while adjacencies are being re-established or the router is being restarted (range is 5-1,800; default is 120). • **Max Neighbor Restart Time**—Maximum grace period, in seconds, that the firewall will accept as a help-mode router. If the peer devices offers

OSPF – Advanced Settings	Description
	a longer grace period in its grace LSA, the firewall will not enter helper mode (range is 5-1,800; default is 140).

OSPFv3

- Network > Virtual Router > OSPFv3

Configuring the Open Shortest Path First v3 (OSPFv3) protocol requires configuring the first three settings in the following table (BFD is optional):

OSPFv3 Settings	Description
Enable	Select to enable the OSPF protocol.
Reject Default Route	Select if you do not want to learn any default routes through OSPF.
Router ID	Specify the router ID associated with the OSPF instance in this virtual router. The OSPF protocol uses the router ID to uniquely identify the OSPF instance.
BFD	To enable Bidirectional Forwarding Detection (BFD) for OSPFv3 globally for the virtual router on a PA-5200 Series, PA-7000 Series, and VM-Series firewall, select one of the following: • **default** (default BFD settings) • a BFD profile that you have created on the firewall • **New BFD Profile** to create a new BFD profile Select **None (Disable BFD)** to disable BFD for all OSPFv3 interfaces on the virtual router; you cannot enable BFD for a single OSPFv3 interface.

In addition, configure OSPFv3 settings on the following tabs:

- **Areas**: See OSPFv3 Areas Tab.
- **Auth Profiles**: See OSPFv3 Auth Profiles Tab.
- **Export Rules**: See OSPFv3 Export Rules Tab.
- **Advanced**: See OSPFv3 Advanced Tab.

OSPFv3 Areas Tab

- Network > Virtual Router > OSPFv3 > Areas

Use the following fields to configure OSPFv3 areas.

OSPv3 – Areas Settings	Description
Authentication	Select the name of the Authentication profile that you want to specify for this OSPF area.
Type	Select one of the following:

OSPv3 – Areas Settings	Description
	• **Normal**—There are no restrictions; the area can carry all types of routes. • **Stub**—There is no outlet from the area. To reach a destination outside of the area, it is necessary to go through the border, which connects to other areas. If you select this option, select **Accept Summary** if you want to accept this type of link state advertisement (LSA) from other areas. Also, specify whether to include a default route LSA in advertisements to the stub area along with the associated metric value (1-255). If the **Accept Summary** option on a stub area Area Border Router (ABR) interface is disabled, the OSPF area will behave as a Totally Stubby Area (TSA) and the ABR will not propagate any summary LSAs. • **NSSA** (Not-So-Stubby Area)—It is possible to leave the area directly, but only by routes other than OSPF routes. If you select this option, select **Accept Summary** if you want to accept this type of LSA. Specify whether to include a default route LSA in advertisements to the stub area along with the associated metric value (1-255). Also, select the route type used to advertise the default LSA. Click **Add** in the **External Ranges** section and enter ranges if you want to enable or suppress advertising external routes that are learned through NSSA to other areas
Range	Click **Add** to aggregate LSA destination IPv6 addresses in the area by subnet. Enable or suppress advertising LSAs that match the subnet, and click **OK**. Repeat to add additional ranges.
Interface	Click **Add** and enter the following information for each interface to be included in the area, and click **OK**. • **Interface**—Choose the interface. • **Enable**—Cause the OSPF interface settings to take effect. • **Instance ID** –Enter an OSPFv3 instance ID number. • **Passive**—Select to if you do not want the OSPF interface to send or receive OSPF packets. Although OSPF packets are not sent or received if you choose this option, the interface is included in the LSA database. • **Link type**—Choose **Broadcast** if you want all neighbors that are accessible through the interface to be discovered automatically by multicasting OSPF hello messages, such as an Ethernet interface. Choose **p2p** (point-to-point) to automatically discover the neighbor. Choose **p2mp** (point-to-multipoint) when neighbors must be defined manually. Defining neighbors manually is allowed only for p2mp mode. • **Metric**—Enter the OSPF metric for this interface (0-65,535). • **Priority**—Enter the OSPF priority for this interface (0-255). It is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) according to the OSPF protocol. When the value is zero, the router will not be elected as a DR or BDR.

OSPv3 – Areas Settings	Description
	• **Auth Profile**—Select a previously-defined authentication profile. • **BFD**—To enable Bidirectional Forwarding Detection (BFD) for an OSPFv3 peer interface (and thereby override the **BFD** setting for OSPFv3, as long as **BFD** is not disabled for OSPFv3 at the virtual router level), select one of the following: • **default** (default BFD settings) • a BFD profile that you have created on the firewall • **New BFD Profile** to create a new BFD profile Select **None (Disable BFD)** to disable BFD for the OSPFv3 peer interface. • **Hello Interval (sec)**—Interval, in seconds, at which the OSPF process sends hello packets to its directly connected neighbors (range is 0-3,600; default is 10). • **Dead Counts**—Number of times the hello interval can occur for a neighbor without OSPF receiving a hello packet from the neighbor, before OSPF considers that neighbor down. The **Hello Interval** multiplied by the **Dead Counts** equals the value of the dead timer (range is 3-20; default is 4). • **Retransmit Interval (sec)**—Length of time, in seconds, that OSPF waits to receive a link-state advertisement (LSA) from a neighbor before OSPF retransmits the LSA (range is 0-3,600; default is 10). • **Transit Delay (sec)**—Length of time, in seconds, that an LSA is delayed before the firewall sends it out of an interface (range is 0-3,600; default is 1).
Interface (continued)	• **Graceful Restart Hello Delay (sec)**—Applies to an OSPF interface when Active/Passive High Availability is configured. **Graceful Restart Hello Delay** is the length of time during which the firewall sends Grace LSA packets at 1-second intervals. During this time, no hello packets are sent from the restarting firewall. During the restart, the dead timer (which is the **Hello Interval** multiplied by the **Dead Counts**) is also counting down. If the dead timer is too short, the adjacency will go down during the graceful restart because of the hello delay. Therefore, it is recommended that the dead timer be at least four times the value of the **Graceful Restart Hello Delay**. For example, a **Hello Interval** of 10 seconds and a **Dead Counts** of 4 yield a dead timer of 40 seconds. If the **Graceful Restart Hello Delay** is set to 10 seconds, that 10-second delay of hello packets is comfortably within the 40-second dead timer, so the adjacency will not time out during a graceful restart (range is 1-10; default is 10). • **Neighbors**—For p2pmp interfaces, enter the neighbor IP address for all neighbors that are reachable through this interface.
Virtual Links	Configure the virtual link settings to maintain or enhance backbone area connectivity. The settings must be defined for area boarder routers, and must be defined within the backbone

OSPv3 – Areas Settings	Description
	area (0.0.0.0). Click **Add**, enter the following information for each virtual link to be included in the backbone area, and click **OK**. • **Name**—Enter a name for the virtual link. • **Instance ID**—Enter an OSPFv3 instance ID number. • **Neighbor ID**—Enter the router ID of the router (neighbor) on the other side of the virtual link. • **Transit Area**—Enter the area ID of the transit area that physically contains the virtual link. • **Enable**—Select to enable the virtual link. • **Timing**—It is recommended that you keep the default timing settings. • **Auth Profile**—Select a previously-defined authentication profile.

OSPFv3 Auth Profiles Tab

- Network > Virtual Router > OSPFv3 > Auth Profiles

Use the following fields to configure authentication for OSPFv3.

OSPFv3 – Auth Profile Settings	Description
Profile Name	Enter a name for the authentication profile. To authenticate the OSPF messages, first define the authentication profiles and then apply them to interfaces on the **OSPF** tab.
SPI	Specify the security parameter index (SPI) for packet traversal from the remote firewall to the peer.
Protocol	Specify either of the following protocols: • **ESP**—Encapsulating Security Payload protocol. • **AH**—Authentication Header protocol
Crypto Algorithm	Specify one of the following • **None**—No crypto algorithm will be used. • **SHA1** (default)—Secure Hash Algorithm 1. • **SHA256**—Secure Hash Algorithm 2. A set of four hash functions with a 256 bit digest. • **SHA384**—Secure Hash Algorithm 2. A set of four hash functions with a 384 bit digest. • **SHA512**—Secure Hash Algorithm 2. A set of four hash functions with a 512 bit digest. • **MD5**—The MD5 message-digest algorithm.
Key/Confirm Key	Enter and confirm an authentication key.

OSPFv3 – Auth Profile Settings	Description
Encryption (ESP protocol only)	Specify one of the following: • **3des** (default)—applies Triple Data Encryption Algorithm (3DES) using three cryptographic keys of 56 bits. • **aes-128-cbc**—applies the Advanced Encryption Standard (AES) using cryptographic keys of 128 bits. • **aes-192-cbc**—applies the Advanced Encryption Standard (AES) using cryptographic keys of 192 bits. • **aes-256-cbc**—applies the Advanced Encryption Standard (AES) using cryptographic keys of 256 bits. • **null**—No encryption is used.
Key/Confirm Key	Enter and confirm an encryption key.

OSPFv3 Export Rules Tab

- Network > Virtual Router > OSPFv3 > Export Rules

Use the following fields to export OSPFv3 routes.

OSPFv3 – Export Rules Settings	Description
Allow Redistribute Default Route	Select to permit redistribution of default routes through OSPF.
Name	Select the name of a redistribution profile. The value must be an IP subnet or valid redistribution profile name.
New Path Type	Choose the metric type to apply.
New Tag	Specify a tag for the matched route that has a 32-bit value.
Metric	(Optional) Specify the route metric to be associated with the exported route and used for path selection (range is 1-65,535).

OSPFv3 Advanced Tab

- Network > Virtual Router > OSPFv3 > Advanced

Use the following fields to disable transit routing for SPF calculations, configure OSPFv3 timers, and configure graceful restart for OSPFv3.

OSPFv3 – Advanced Settings	Description
Disable Transit Routing for SPF Calculation	Select if you want to set the R-bit in router LSAs sent from this firewall to indicate that the firewall is not active. When in this state, the firewall participates in OSPFv3 but other routers do not send transit traffic. In this state, local traffic will still be forwarded to the firewall. This is useful while performing maintenance with a dual-homed network because traffic can be re-routed around the firewall while it can still be reached.
Timers	• **SPF Calculation Delay (sec)**—This is a delay timer allowing you to tune the delay time between receiving new topology information and performing an SPF calculation. Lower values enable faster OSPF re-convergence. Routers peering with the firewall should be tuned in a similar manner to optimize convergence times. • **LSA Interval (sec)**—The option specifies the minimum time between transmissions of two instances of the same LSA (same router, same type, same LSA ID). This is equivalent to MinLSInterval in RFC 2328. Lower values can be used to reduce re-convergence times when topology changes occur.
Graceful Restart	• **Enable Graceful Restart**—Enabled by default, a firewall enabled for this feature will instruct neighboring routers to continue using a route through the firewall while a transition takes place that renders the firewall temporarily down. • **Enable Helper Mode**—Enabled by default, a firewall enabled for this mode continues to forward to an adjacent device when that device is restarting. • **Enable Strict LSA Checking**—Enabled by default, this feature causes an OSPF helper mode enabled firewall to exit helper mode if a topology change occurs. • **Grace Period (sec)**—The period of time, in seconds, that peer devices continue to forward to this firewall while adjacencies are being re-established or while the router is being restarted (range is 5-1,800; default is 120). • **Max Neighbor Restart Time**—The maximum grace period, in seconds, that the firewall will accept as a help-mode router. If the peer devices offers a longer grace period in its grace LSA, the firewall will not enter helper mode (range is 5-800; default is 140).

BGP

- Network > Virtual Router > BGP

Configuring Border Gateway Protocol (BGP) requires you to configure Basic BGP Settings to enable BGP and configure the Router ID and AS Number as described in the following table. In addition, you must configure a BGP peer as part of a BGP peer group.

Configure the remaining BGP settings on the following tabs as needed for your network:

- **General**: See BGP General Tab.

- **Advanced**: See BGP Advanced Tab.
- **Peer Group**: See BGP Peer Group Tab.
- **Import**: See BGP Import and Export Tabs.
- **Export**: See BGP Import and Export Tabs.
- **Conditional Adv**: See BGP Conditional Adv Tab.
- **Aggregate**: See BGP Aggregate Tab.
- **Redist Rules**: See BGP Redist Rules Tab.

Basic BGP Settings

To use BGP on a virtual router, you must enable BGP and configure the Router ID and AS Number; enabling BFD is optional.

BGP Settings	Configure In	Description
Enable	**BGP**	Select to enable BGP.
Router ID		Enter the IP address to assign to the virtual router.
AS Number		Enter the number of the AS to which the virtual router belongs, based on the router ID (range is 1 to 4,294,967,295).
BFD		To enable Bidirectional Forwarding Detection (BFD) for BGP globally for the virtual router on a PA-5200 Series, PA-7000 Series, or VM-Series firewall, select one of the following: • **default** (default BFD settings) • an existing BFD profile on the firewall • create a **New BFD Profile** Select **None (Disable BFD)** to disable BFD for all BGP interfaces on the virtual router; you cannot enable BFD for a single BGP interface. *If you enable or disable BFD globally, all interfaces running BGP are taken down and brought back up with the BFD function, which can disrupt BGP traffic. Therefore, enable BFD on BGP interfaces during an off-peak time when reconvergence does not impact production traffic.*

BGP General Tab

- Network > Virtual Router > BGP > General

Use the following fields to configure general BGP settings.

BGP General Settings	Configure In	Description
Reject Default Route	**BGP** > **General**	Select to ignore any default routes that are advertised by BGP peers.

BGP General Settings	Configure In	Description
Install Route		Select to install BGP routes in the global routing table.
Aggregate MED		Select to enable route aggregation even when routes have different Multi-Exit Discriminator (MED) values.
Default Local Preference		Specifies a value that the firewall can use to determine preferences among different paths.
AS Format		Select the 2-byte (default) or 4-byte format. This setting is configurable for interoperability purposes.
Always Compare MED		Enable MED comparison for paths from neighbors in different autonomous systems.
Deterministic MED Comparison		Enable MED comparison to choose between routes that are advertised by iBGP peers (BGP peers in the same autonomous system).
Auth Profiles		**Add** a new auth profile and configure the following settings: • **Profile Name**—Enter a name to identify the profile. • **Secret/Confirm Secret**—Enter and confirm a passphrase for BGP peer communications. Delete (⊖) profiles when you no longer need them.

BGP Advanced Tab

- Network > Virtual Router > BGP > Advanced

Advanced BGP settings include a variety of capabilities. You can run ECMP over multiple BGP autonomous systems. You can require eBGP peers to list their own AS as the first AS in an AS_PATH attribute (to prevent spoofed Update packets). You can configure BGP graceful restart, a means by which BGP peers indicate whether they can preserve forwarding state during a BGP restart to minimize the consequences of routes flapping (going up and down). You can configure route reflectors and AS confederations, which are two methods to avoid having a full mesh of BGP peerings in an AS. You can configure route dampening to prevent unnecessary router convergence when a BGP network is unstable and routes are flapping.

BGP Advanced Settings	Configure In	Description
ECMP Multiple AS Support	**BGP** > **Advanced**	Select if you enable ECMP for a virtual router and you want to run ECMP over multiple BGP autonomous systems.
Enforce First AS for EBGP		Causes the firewall to drop an incoming Update packet from an eBGP peer that doesn't list the eBGP peer's own AS number as the first AS number in the AS_PATH attribute. This prevents BGP from further processing a spoofed or erroneous Update packet that arrives from an AS other than a neighboring AS. Default is enabled.

BGP Advanced Settings	Configure In	Description
Graceful Restart		Activate the graceful restart option. • **Stale Route Time**—Specify the length of time, in seconds, that a route can stay in the stale state (range is 1-3,600; default is 120). • **Local Restart Time**—Specify the length of time, in seconds, that the firewall takes to restart. This value is advertised to peers (range is 1-3,600; default is 120). • **Max Peer Restart Time**—Specify the maximum length of time, in seconds, that the firewall accepts as a grace period restart time for peer devices (range is 1-3,600; default is 120).
Reflector Cluster ID		Specify an IPv4 identifier to represent the reflector cluster. A route reflector (router) in an AS performs a role of re-advertising routes it learned to its peers (rather than require full mesh connectivity and all peers send routes to each other). The route reflector simplifies configuration.
Confederation Member AS		Specify the autonomous system number identifier that is visible only within the BGP confederation (also called a sub-autonomous system number). Use a BGP confederation to divide autonomous systems into sub-autonomous systems and reduce full mesh peering.
Dampening Profiles	**BGP > Advanced (cont)**	Route dampening is a method that determine whether a route is suppressed from being advertised because it is flapping. Route dampening can reduce the number of times routers are forced to reconverge due to routes flapping. Settings include: • **Profile Name**—Enter a name to identify the profile. • **Enable**—Activate the profile. • **Cutoff**—Specify a route withdrawal threshold above which a route advertisement is suppressed (range is 0.0-1,000.0; default is 1.25). • **Reuse**—Specify a route withdrawal threshold below which a suppressed route is used again (range is 0.0-1,000.0; default is 5). • **Max. Hold Time**—Specify the maximum length of time, in seconds, that a route can be suppressed, regardless of how unstable it has been (range is 0-3,600; default is 900). • **Decay Half Life Reachable**—Specify the length of time, in seconds, after which a route's stability metric is halved if the firewall considers the route is reachable (range is 0-3,600; default is 300). • **Decay Half Life Unreachable**—Specify the length of time, in seconds, after which a route's stability metric is halved if the firewall considers the route is unreachable (range is 0-3,600; default is 300). Delete (⊖) profiles when you no longer need them.

BGP Peer Group Tab

- Network > Virtual Router > BGP > Peer Group

A BGP peer group is a collection of BGP peers that share settings, such as the type of peer group (EBGP, for example), or the setting to remove private AS numbers from the AS_PATH list that the virtual router sends in Update packets. BGP peer groups save you from having to configure multiple peers with the same settings. You must configure at least one BGP peer group in order to configure the BGP peers that belong to the group.

BGP Peer Group Settings	Configure In	Description
Name	**BGP** > **Peer Group**	Enter a name to identify the peer group.
Enable		Select to activate the peer group.
Aggregated Confed AS Path		Select to include a path to the configured aggregated confederation AS.
Soft Reset with Stored Info		Select to perform a soft reset of the firewall after updating the peer settings.
Type		Specify the type of peer or group and configure the associated settings (see below in this table for descriptions of **Import Next Hop** and **Export Next Hop**). • **IBGP**—Specify the following: • **Export Next Hop** • **EBGP Confed**—Specify the following: • **Export Next Hop** • **IBGP Confed**—Specify the following: • **Export Next Hop** • **EBGP**—Specify the following: • **Import Next Hop** • **Export Next Hop** • **Remove Private AS** (select if you want to force BGP to remove private AS numbers from the AS_PATH attribute).
Import Next Hop		Choose an option for next hop import: • **Original**—Use the Next Hop address provided in the original route advertisement. • **Use Peer**—Use the peer's IP address as the Next Hop address.
Export Next Hop		Choose an option for next hop export: • **Resolve**—Resolve the Next Hop address using the Forwarding Information Base (FIB). • **Original**—Use the Next Hop address provided in the original route advertisement.

BGP Peer Group Settings	Configure In	Description
		• **Use Self**—Replace the Next Hop address with the virtual router's IP address to ensure that it will be in the forwarding path.
Remove Private AS		Select to remove private autonomous systems from the AS_PATH list.
Name	**BGP** > **Peer Group** > **Peer**	Add a **New** BGP peer and enter a name to identify it.
Enable		Select to activate the peer.
Peer AS		Specify the autonomous system (AS) of the peer.
Enable MP-BGP Extensions	**BGP** > **Peer Group** > **Peer** > **Addressing**	Enables the firewall to support the Multiprotocol BGP Address Family Identifier for IPv4 and IPv6 and Subsequent Address Family Identifier options per RFC 4760.
Address Family Type		Select either the **IPv4** or **IPv6** address family that BGP sessions with this peer will support.
Subsequent Address Family		Select either the **Unicast** or **Multicast** subsequent address family protocol the BGP sessions with this peer will carry.
Local Address —Interface		Choose a firewall interface.
Local Address —IP		Choose a local IP address.
Peer Address —Type and Address		Select the type of address that identifies the peer: • **IP**—Select IP and select an address object that uses an IP address (or create a new address object that uses an IP address). • **FQDN**—Select FQDN and select an address object that uses an FQDN (or create a new address object that uses an FQDN).
Auth Profile	**BGP** > **Peer Group** > **Peer** > **Connection Options**	Select a profile or select **New Auth Profile** from the drop down. Enter a Profile **Name** and the **Secret**, and **Confirm Secret**.
Keep Alive Interval		Specify an interval after which routes from a peer are suppressed according to the hold time setting (range is 0-1,200 seconds; default is 30 seconds).
Multi Hop		Set the time-to-live (TTL) value in the IP header (range is 0 to 255; default is 0). The default value of 0 means 1 for eBGP. The default value of 0 means 255 for iBGP.
Open Delay Time		Specify the delay time between opening the peer TCP connection and sending the first BGP open message (range is 0-240 seconds; default is 0 seconds).
Hold Time		Specify the period of time that may elapse between successive KEEPALIVE or UPDATE messages from a peer before the peer

BGP Peer Group Settings	Configure In	Description
		connection is closed (range is 3-3,600 seconds; default is 90 seconds).
Idle Hold Time		Specify the time to wait in the idle state before retrying connection to the peer (range is 1-3,600 seconds; default is 15 seconds).
Incoming Connections—Remote Port		Specify the incoming port number and **Allow** traffic to this port.
Outgoing Connections—Local Port		Specify the outgoing port number and **Allow** traffic from this port
Reflector Client	**BGP** > **Peer Group** > **Peer** > **Advanced**	Select the type of reflector client (**Non-Client**, **Client**, or **Meshed Client**). Routes that are received from reflector clients are shared with all internal and external BGP peers.
Peering Type		Specify a Bilateral peer or leave Unspecified.
Max Prefixes		Specify the maximum number of supported IP prefixes (1#100,000 or unlimited).
Enable Sender Side Loop Detection		Enable to cause the firewall to check the AS_PATH attribute of a route in its FIB before it sends the route in an update, to ensure that the peer AS number is not on the AS_PATH list. If it is, the firewall removes it to prevent a loop. Usually the receiver does loop detection, but this optimization feature has the sender do loop detection.
BFD		To enable Bidirectional Forwarding Detection (BFD) for a BGP peer (and thereby override the **BFD** setting for BGP, as long as **BFD** is not disabled for BGP at the virtual router level), select the default profile (default BFD settings), an existing BFD profile, **Inherit-vr-global-setting** (to inherit the global BGP BFD profile), or **New BFD Profile** (to create a new BFD profile). **Disable BFD** disables BFD for the BGP peer. *If you enable or disable BFD globally, all interfaces running BGP will be taken down and brought back up with the BFD function. This can disrupt all BGP traffic. When you enable BFD on the interface, the firewall will stop the BGP connection to the peer to program BFD on the interface. The peer device will see the BGP connection drop, which can result in a reconvergence that impacts production traffic. Therefore, enable BFD on BGP interfaces during an off-peak time when a reconvergence will not impact production traffic.*

BGP Import and Export Tabs

- Network > Virtual Router > BGP > Import
- Network > Virtual Router > BGP > Export

Add a new Import or Export rule to import or export BGP routes.

BGP Import and Export Settings	Configure In	Description
Rules	**BGP** > **Import or Export** > **General**	Specify a name to identify the rule.
Enable		Select to activate the rule.
Used By		Select the peer groups that will use this rule.
AS-Path Regular Expression	**BGP** > **Import or Export** > **Match**	Specify a regular expression for filtering of AS paths.
Community Regular Expression		Specify a regular expression for filtering of community strings.
Extended Community Regular Expression		Specify a regular expression for filtering of extended community strings.
MED		Specify a Multi-Exit Discriminator value for route filtering in the range 0-4,294,967,295.
Route Table		For an **Import Rule**, specify which route table the matching routes will be imported into: **unicast**, **multicast**, or **both**. For an **Export Rule**, specify which route table the matching routes will be exported from: **unicast**, **multicast**, or **both**.
Address Prefix		Specify IP addresses or prefixes for route filtering.
Next Hop		Specify next hop routers or subnets for route filtering
From Peer		Specify peer routers for route filtering
Action	**BGP** > **Import or Export** > **Action**	Specify an action (**Allow** or **Deny**) to take when the match conditions are met.
Dampening		Specify the dampening parameter, only if the action is **Allow**.
Local Preference		Specify a local preference metric, only if the action is **Allow**.
MED		Specify a MED value, only if the action is **Allow** (0- 65,535).

BGP Import and Export Settings	Configure In	Description
Weight		Specify a weight value, only if the action is **Allow** (0- 65,535).
Next Hop		Specify a next hop router, only if the action is **Allow**.
Origin		Specify the path type of the originating route: IGP, EGP, or incomplete, only if the action is **Allow**.
AS Path Limit		Specify an AS path limit, only if the action is **Allow**.
AS Path		Specify an AS path: **None**, **Remove**, **Prepend**, **Remove and Prepend**, only if the action is **Allow**.
Community		Specify a community option: **None**, **Remove All**, **Remove Regex**, **Append**, or **Overwrite**, only if the action is **Allow**.
Extended Community		Specify a community option: **None**, **Remove All**, **Remove Regex**, **Append**, or **Overwrite**, only if the action is **Allow**.
		Delete ⊖ rules when you no longer need them or **Clone** a rule when appropriate. You can also select rules and **Move Up** or **Move Down** to change their order.

BGP Conditional Adv Tab

- Network > Virtual Router > BGP > Conditional Adv

A BGP conditional advertisement allows you to control which route to advertise in the event that a preferred route is not available in the local BGP routing table (LocRIB), indicating a peering or reachability failure. This is useful where you want to try to force routes to one AS over another, such as when you have links to the internet through multiple ISPs and you want traffic to be routed to one provider instead of the other except when there is a loss of connectivity to the preferred provider.

For conditional advertisement, you configure a Non Exist filter that specifies the preferred route(s) (**Address Prefix**) plus any other attributes that identify the preferred route (such as AS Path Regular Expression). If a route matching the Non Exist filter is not found in the local BGP routing table, only then will the firewall allow advertisement of the alternate route (the route to the other, non-preferred provider) as specified in its Advertise filter.

To configure conditional advertisement, select the **Conditional Adv** tab, **Add** a conditional advertisement, and configure the values described in the following table.

BGP Conditional Advertisement Settings	Configure In	Description
Policy	**BGP** > **Conditional Adv**	Specify a name for this conditional advertisement policy rule.
Enable		Select to enable this conditional advertisement policy rule.

BGP Conditional Advertisement Settings	Configure In	Description
Used By		**Add** the peer groups that will use this conditional advertisement policy rule.
Non Exist Filter	**BGP** > **Conditional Adv** > **Non Exist Filters**	Use this tab to specify the prefix(es) of the preferred route. This specifies the route that you want to advertise, if it is available in the local BGP routing table. (If a prefix is going to be advertised and matches a Non Exist filter, the advertisement will be suppressed.) **Add** a Non Exist Filter and specify a name to identify this filter.
Enable		Select to activate the Non Exist filter.
AS Path Regular Expression		Specify a regular expression for filtering AS paths.
Community Regular Expression		Specify a regular expression for filtering community strings.
Extended Community Regular Expression		Specify a regular expression for filtering extended community strings.
MED		Specify a MED value for route filtering (range is 0-4,294,967,295).
Route Table		Specify which route table (**unicast**, **multicast**, or **both**) the firewall will search to see if the matched route is present. If the matched route is not present in that route table, only then will the firewall allow the advertisement of the alternate route.
Address Prefix		**Add** the exact Network Layer Reachability Information (NLRI) prefix for the preferred route(s).
Next Hop		Specify next hop routers or subnets for filtering the route.
From Peer		Specify peer routers for route filtering.
Advertise Filter	**BGP** > **Conditional Adv** > **Advertise Filters**	Use this tab to specify the prefix(es) of the route in the Local-RIB routing table to advertise if the route in the Non Exist filter is not available in the local routing table. If a prefix is to be advertised and does not match a Non Exist filter, the advertisement will occur. **Add** an advertise filter and specify a name to identify this filter.
Enable		Select to activate the filter.

BGP Conditional Advertisement Settings	Configure In	Description
AS Path Regular Expression		Specify a regular expression for filtering AS paths.
Community Regular Expression		Specify a regular expression for filtering community strings.
Extended Community Regular Expression		Specify a regular expression for filtering extended community strings.
MED		Specify a MED value for route filtering (range is 0-4,294,967,295).
Route Table		Specify which route table the firewall uses when a matched route is to be conditionally advertised: **unicast**, **multicast**, or **both**.
Address Prefix		**Add** the exact Network Layer Reachability Information (NLRI) prefix for the route to be advertised if the preferred route is not available.
Next Hop		Specify next hop routers or subnets for route filtering.
From Peer		Specify peer routers for route filtering.

BGP Aggregate Tab

- Network > Virtual Router > BGP > Aggregate

Route aggregation is the act of combining specific routes (those with a longer prefix length) into a single route (with a shorter prefix length) to reduce routing advertisements that the firewall must send and to have fewer routes in the route table.

BGP Aggregate Settings	Configure In	Description
Name	**BGP** > **Aggregate**	Enter a name for the aggregation rule.
Prefix		Enter a summary prefix (IP address/prefix length) that will be used to aggregate the longer prefixes.
Enable		Select to enable this aggregation of routes.
Summary		Select to summarize routes.
AS Set		Select to cause the firewall, for this aggregation rule, to include the set of AS numbers (AS set) in the AS path of the aggregate route.

BGP Aggregate Settings	Configure In	Description
		The AS set is the unordered list of the origin AS numbers from the individual routes that are aggregated.
Name	**BGP** > **Aggregate** > **Suppress Filters**	Define the attributes that will cause the matched routes to be suppressed. **Add** and enter a name for a Suppress Filter.
Enable		Select to enable the Suppress Filter.
AS Path Regular Expression		Specify a regular expression for AS_PATH to filter which routes will be aggregated, for example, ^5000 means routes learned from AS 5000.
Community Regular Expression		Specify a regular expression for communities to filter which routes will be aggregated, for example, 500:.* matches communities with 500:x.
Extended Community Regular Expression		Specify a regular expression for extended communities to filter which routes will be aggregated.
MED		Specify the MED that filters which routes will be aggregated.
Route Table		Specify which route table to use for aggregated routes that should be suppressed (not advertised): **unicast**, **multicast**, or **both**.
Address Prefix		Enter the IP address that you want to suppress from advertisement.
Next Hop		Enter the next hop address of the BGP prefix that you want to suppress.
From Peer		Enter the IP address of the peer from which the BGP prefix (that you want to suppress) was received.
Name	**BGP** > **Aggregate** > **Advertise Filters**	Define the attributes for an Advertise Filter that causes the firewall to advertise to peers any route that matches the filter. Click **Add** and enter a name for the Advertise Filter.
Enable		Select to enable this Advertise Filter.
AS Path Regular Expression		Specify a regular expression for AS_PATH to filter which routes will be advertised.
Community Regular Expression		Specify a regular expression for Community to filter which routes will be advertised.
Extended Community		Specify a regular expression for Extended Community to filter which routes will be advertised.

BGP Aggregate Settings	Configure In	Description
Regular Expression		
MED		Specify a MED value to filter which routes will be advertised.
Route Table		Specify which route table to use for an Advertise Filter of aggregate routes: **unicast**, **multicast**, or **both**.
Address Prefix		Enter an IP address that you want BGP to advertise.
Next Hop		Enter the Next Hop address of the IP address you want BGP to advertise.
From Peer		Enter the IP address of the peer from which the prefix was received, that you want BGP to advertise.
	BGP > **Aggregate** > **Aggregate Route Attributes**	Define the attributes for the aggregate route.
Local Preference		Local preference in the range 0-4,294,967,295.
MED		Multi Exit Discriminator in the range 0-4,294,967,295.
Weight		Weight in the range 0-65,535.
Next Hop		Next Hop IP address.
Origin		Origin of the route: **igp**, **egp**, or **incomplete**.
AS Path Limit		AS Path Limit in the range 1-255.
AS Path		Select Type: **None** or **Prepend**.
Community		Select Type: **None**, **Remove All**, **Remove Regex**, **Append**, or **Overwrite**.
Extended Community		Select Type: **None**, **Remove All**, **Remove Regex**, **Append**, or **Overwrite**.

BGP Redist Rules Tab

- Network > Virtual Router > BGP > Redist Rules

Configure the settings described in the following table to create rules for redistributing BGP routes.

BGP Redistribution Rules Settings	Configure In	Description
Allow Redistribute Default Route	**BGP** > **Redist Rules**	Permits the firewall to redistribute its default route to BGP peers.
Name		**Add** an IP subnet or create a redistribution rule first.
Enable		Select to enable this redistribution rule.
Route Table		Specify which route table the route will be redistributed into: **unicast**, **multicast**, or **both**.
Metric		Enter a metric in the range 1-65,535.
Set Origin		Select the origin for the redistributed route (**igp**, **egp**, or **incomplete**). The value **incomplete** indicates a connected route.
Set MED		Enter a MED for the redistributed route in the range 0-4,294,967,295.
Set Local Preference		Enter a local preference for the redistributed route in the range 0-4,294,967,295.
Set AS Path Limit		Enter an AS path limit for the redistributed route in the range 1-255.
Set Community		Select or enter a 32-bit value in decimal or hexadecimal or in AS:VAL format; AS and VAL are each in the range 0-65,535. Enter a maximum of 10 communities.
Set Extended Community		Enter a 64-bit value in hexadecimal or in TYPE:AS:VAL or TYPE:IP:VAL format. TYPE is 16 bits; AS or IP is 16 bits; VAL is 32 bits. Enter a maximum of five extended communities.

IP Multicast

- Network > Virtual Router > Multicast

Configuring Multicast protocols requires configuring the following standard setting:

Multicast Setting	Description
Enable	Select to enable multicast routing.

In addition, settings on the following tabs must be configured:

- **Rendezvous Point**: See Multicast Rendezvous Point Tab.
- **Interfaces**: See Multicast Interfaces Tab.
- **SPT Threshold**: See Multicast SPT Threshold Tab.

- **Source Specific Address Space**: See Multicast Source Specific Address Tab.
- **Advanced**: See Multicast Advanced Tab.

Multicast Rendezvous Point Tab

- Network > Virtual Router > Multicast > Rendezvous Point

Use the following fields to configure an IP multicast rendezvous point:

Multicast Settings – Rendezvous Point	Description
RP Type	Choose the type of Rendezvous Point (RP) that will run on this virtual router. A static RP must be explicitly configured on other PIM routers whereas a candidate RP is elected automatically. • **None**—Choose if there is no RP running on this virtual router. • **Static**—Specify a static IP address for the RP and choose options for **RP Interface** and **RP Address** from the drop-down. Select **Override learned RP for the same group** if you want to use the specified RP instead of the RP elected for this group. • **Candidate**—Specify the following information for the candidate RP running on this virtual router: • **RP Interface**—Select an interface for the RP. Valid interface types include loopback, L3, VLAN, aggregate Ethernet, and tunnel. • **RP Address**—Select an IP address for the RP. • **Priority**—Specify a priority for candidate RP messages (default 192). • **Advertisement interval**—Specify an interval between advertisements for candidate RP messages. • **Group list**—If you choose **Static** or **Candidate**, click **Add** to specify a list of groups for which this candidate RP is proposing to be the RP.
Remote Rendezvous Point	Click **Add** and specify the following: • **IP address**—Specify the IP address for the RP. • **Override learned RP for the same group**—Select to use the specified RP instead of the RP elected for this group. • **Group**—Specify a list of groups for which the specified address will act as the RP.

Multicast Interfaces Tab

- Network > Virtual Router > Multicast > Interfaces

Use the following fields to configure multicast interfaces that share IGMP, PIM and group permission settings:

Multicast Settings – Interfaces	Description
Name	Enter a name to identify an interface group.

Multicast Settings – Interfaces	Description
Description	Enter an optional description.
Interface	**Add** one or more firewall interfaces that belong to the interface group and therefore share multicast group permissions, IGMP settings and PIM settings.
Group Permissions	Specify multicast groups that participate in PIM Any-Source Multicast (ASM) or PIM Source-Specific Multicast (SSM): • **Any Source**—**Add** a **Name** to identify a multicast **Group** that is allowed to receive multicast traffic from any source on the interfaces in the interface group. By default the group is **Included** in the **Any Source** list. Deselect **Included** to easily exclude a group without deleting the group configuration. • **Source Specific**—**Add** a **Name** for a multicast **Group** and **Source** IP address pair for which multicast traffic is allowed on the interfaces in the interface group. By default the Group and Source pair is **Included** in the Source Specific list. Deselect **Included** to easily exclude a Group and Source pair without deleting the configuration.
IGMP	Specify settings for IGMP traffic. IGMP must be enabled for multicast receiver-facing interfaces. • **Enable**—Select to enable the IGMP configuration. • **IGMP Version**—Choose version 1, 2, or 3 to run on the interface. • **Enforce Router-Alert IP Option**—Select to require the router-alert IP option when speaking IGMPv2 or IGMPv3. This must be disabled for compatibility with IGMPv1. • **Robustness**—Choose an integer value to account for packet loss on a network (range is 1 to 7; default is 2). If packet loss is common, choose a higher value. • **Max Sources**—Specify the maximum number of source-specific memberships allowed for the interface group (range is 1 to 65,535 or **unlimited**). • **Max Groups**—Specify the maximum number of multicast groups allowed for this interface group (range is 1 to 65,535 or **unlimited**). • **Query Configuration**—Specify the following: • **Query Interval**—Specify the interval at which general queries are sent to all receivers. • **Max Query Response Time**—Specify the maximum time between a general query and a response from a receiver. • **Last Member Query Interval**—Specify the interval between group or source-specific query messages (including those sent in response to leave-group messages). • **Immediate Leave**—Select to leave the group immediately when a leave message is received.
PIM configuration	Specify Protocol Independent Multicast (PIM) settings: • **Enable**—Select to allow this interface to receive and/or forward PIM messages. You must enable for an interface to forward multicast traffic.

Multicast Settings – Interfaces	Description
	• **Assert Interval**—Specify the interval between PIM assert messages to elect a PIM Forwarder. • **Hello Interval**—Specify the interval between PIM hello messages. • **Join Prune Interval**—Specify the number of seconds between PIM join messages (and between PIM prune messages). Default is 60. • **DR Priority**—Specify the designated router priority for this interface. • **BSR Border**—Select to use the interface as the bootstrap border. • **PIM Neighbors**—**Add** the list of neighbors that will communicate using PIM.

Multicast SPT Threshold Tab

- Network > Virtual Router > Multicast > SPT Threshold

The Shortest Path Tree (SPT) threshold defines the point at which the virtual router switches multicast routing for a multicast group or prefix from shared tree distribution (sourced from the rendezvous point) to source tree (also known as shortest path tree or SPT) distribution. **Add** an SPT threshold for a multicast group or prefix.

SPT Threshold	Description
Multicast Group/Prefix	Specify the multicast address or prefix for which multicast routing switches to SPT distribution when throughput to the group or prefix reaches the threshold setting.
Threshold (kbps)	Select a setting to specify the point at which multicast routing switches to SPT distribution for the corresponding multicast group or prefix: • **0 (switch on first data packet)**—(default) When a multicast packet for the group or prefix arrives, the virtual router switches to SPT distribution. • **never (do not switch to spt)**—The virtual router continues to forward multicast traffic to this group or prefix down the shared tree. • Enter the total number of kilobits from multicast packets that can arrive for the corresponding multicast group or prefix at any interface and over any time period (range is 1 to 4,294,967,295). When throughput reaches this number, the virtual router switches to SPT distribution.

Multicast Source Specific Address Space Tab

- Network > Virtual Router > Multicast > Source Specific Address Space

Add the multicast groups that can receive multicast packets from a specific source only. These are the same multicast groups and names that you specified as Source Specific on the **Multicast** > **Interfaces** > **Group Permissions** tab.

Multicast Settings – Source Specific Address Space	Description
Name	Identify a multicast group for which the firewall provides source-specific multicast (SSM) services.
Group	Specify a multicast group address that can accept multicast packets from a specific source only.
Included	Select to include the multicast group in the SSM address space.

Multicast Advanced Tab

- Network > Virtual Router > Multicast > Advanced

Configure the length of time a multicast route remains in the routing table after the session ends.

Multicast Advanced Settings	Description
Route Age Out Time (sec)	Allows you to tune the duration, in seconds, for which a multicast route remains in the routing table on the firewall after the session ends (range is 210-7200; default is 210).

ECMP

- Network > Virtual Routers > Router Settings > ECMP

Equal Cost Multiple Path (ECMP) processing is a networking feature that enables the firewall to use up to four equal-cost routes to the same destination. Without this feature, if there are multiple equal-cost routes to the same destination, the virtual router chooses one of those routes from the routing table and adds it to its forwarding table; it will not use any of the other routes unless there is an outage in the chosen route. Enabling ECMP functionality on a virtual router allows the firewall have up to four equal-cost paths to a destination in its forwarding table, allowing the firewall to:

- Load balance flows (sessions) to the same destination over multiple equal-cost links.
- Make use of the available bandwidth on all links to the same destination rather than leave some links unused.
- Dynamically shift traffic to another ECMP member to the same destination if a link fails, rather than waiting for the routing protocol or RIB table to elect an alternative path, which can help reduce down time when links fail.

ECMP load balancing is done at the session level, not at the packet level. This means the firewall chooses an equal-cost path at the start of a new session, not each time the firewall receives a packet.

Enabling, disabling, or changing ECMP on an existing virtual router causes the system to restart the virtual router, which might cause existing sessions to be terminated.

To configure ECMP for a virtual router, select a virtual router and, for **Router Settings**, select the **ECMP** tab and configure the ECMP Settings as described.

What are you looking for?	See:
What are the fields available to configure ECMP?	ECMP Settings
Looking for more?	ECMP

ECMP Settings

- Network > Virtual Routers > Router Settings > ECMP

Use the following fields to configure equal-cost multi-path (ECMP) settings.

ECMP Settings	Description
Enable	**Enable** ECMP.  *Enabling, disabling, or changing ECMP on an existing virtual router causes the system to restart the virtual router, which sometimes results in the termination of existing sessions.*
Symmetric Return	(Optional) Select **Symmetric Return** to cause return packets to egress out the same interface on which the associated ingress packets arrived. This configures the firewall to use the ingress interface when sending return packets instead of the ECMP interface, which means that the **Symmetric Return** setting overrides load balancing. This behavior occurs only for traffic flows from the server to the client.
Strict Source Path	By default, IKE and IPSec traffic originating at the firewall egresses an interface that the ECMP load-balancing method determines. Select **Strict Source Path** to ensure that IKE and IPSec traffic originating at the firewall always egresses the physical interface to which the source IP address of the IPSec tunnel belongs. Enable Strict Source Path when the firewall has more than one ISP providing equal-cost paths to the same destination. The ISPs typically perform a Reverse Path Forwarding (RPF) check (or a different check to prevent IP address spoofing) to confirm that the traffic is egressing the same interface on which it arrived. Because ECMP by default chooses an egress interface based on the configured ECMP method (instead of choosing the source interface as the egress interface), that will not be what the ISP expects and the ISP can block legitimate return traffic. In this use case, enable **Strict Source Path** so that the firewall uses the egress interface that is the interface to which the source IP address of the IPSec tunnel belongs.
Max Path	Select the maximum number of equal-cost paths: (2, 3, or 4) to a destination network that can be copied from the RIB to the FIB (default is 2).
Method	Choose one of the following ECMP load-balancing algorithms to use on the virtual router. ECMP load balancing is done at the session level, not at the packet level. This means that the firewall (ECMP) chooses an equal-cost path at the start of a new session, not each time a packet is received.

ECMP Settings	Description
	• **IP Modulo** (default)—The virtual router load balances sessions using a hash of the source and destination IP addresses in the packet header to determine which ECMP route to use. • **IP Hash**—There are two IP hash methods that determine which ECMP route to use: • If you select **IP Hash**, by default the firewall uses a hash of the source and destination IP addresses. • If you **Use Source Address Only** (available in PAN-OS 8.0.3 and later releases), the firewall ensure that all sessions belonging to the same source IP address always take the same path. • If you also **Use Source/Destination Ports**, the firewall includes the ports in either hash calculation. You can also enter a **Hash Seed** value (an integer) to further randomize load balancing. • **Weighted Round Robin**—You can use this algorithm to take in to consideration different link capacities and speeds. When choosing this algorithm, the Interface dialog opens. **Add** and select an **Interface** to include in the weighted round robin group. For each interface, enter the **Weight** for that interface (range is 1 to 255; default is 100). The higher the weight for a specific equal-cost path, the more often that the equal-cost path is selected for a new session. A higher speed link should be given a higher weight than a slower link so that more of the ECMP traffic goes over the faster link. You can then **Add** another interface and weight. • **Balanced Round Robin**—Distributes incoming ECMP sessions equally across links.

More Runtime Stats for a Virtual Router

After you configure static routes or routing protocols for a virtual router, select **Network** > **Virtual Routers**, and select **More Runtime Stats** in the last column to see detailed information about the virtual router, such as the route table, forwarding table, and the routing protocols and static routes you configured. These windows provide more information than can fit on a single screen for the virtual router. The window displays the following tabs:

- **Routing**: See Routing Tab.
- **RIP**: See RIP Tab.
- **BGP**: See BGP Tab.
- **Multicast**: See Multicast Tab.
- **BFD Summary Information**: See BFD Summary Information Tab.

Routing Tab

The following table describes the virtual router's runtime stats for the Route Table, Forwarding Table, and the Static Route Monitoring table.

Runtime Stat	Description
Route Table	
Route Table	Select **Unicast** or **Multicast** to display either the unicast or multicast route table.

Runtime Stat	Description
Display Address Family	Select **IPv4 Only**, **IPv6 Only**, or **IPv4 and IPv6** (default) to control which group of addresses to display in the table.
Destination	IPv4 address and netmask or IPv6 address and prefix length of networks the virtual router can reach.
Next Hop	IP address of the device at the next hop toward the Destination network. A next hop of 0.0.0.0 indicates the default route.
Metric	Metric for the route. When a routing protocol has more than one route to the same destination network, it prefers the route with the lowest metric value. Each routing protocol uses a different type of metric; for example, RIP uses hop count.
Weight	Weight for the route. For example, when BGP has more than one route to the same destination, it will prefer the route with the highest weight.
Flags	• **A?B**—Active and learned via BGP • **A C**—Active and a result of an internal interface (connected) - Destination = network • **A H**—Active and a result of an internal interface (connected) - Destination = Host only • **A R**—Active and learned via RIP • **A S**—Active and static • **S**—Inactive (because this route has a higher metric) and static • **O1**—OSPF external type-1 • **O2**—OSPF external type-2 • **Oi**—OSPF intra-area • **Oo**—OSPF inter-area
Age	Age of the route entry in the routing table. Static routes have no age.
Interface	Egress interface of the virtual router that will be used to reach the next hop.
Refresh	Click to refresh the runtime stats in the table.

Forwarding Table

The firewall chooses the best route—from the route table (RIB) toward a destination network—to place in the FIB.

Display Address Family	Select **IPv4 Only**, **IPv6 Only**, or **IPv4 and IPv6** (default) to control which route table to display.
Destination	Best IPv4 address and netmask or IPv6 address and prefix length to a network the virtual router can reach, selected from the Route Table.
Next Hop	IP address of the device at the next hop toward the Destination network. A next hop of 0.0.0.0 indicates the default route.

Runtime Stat	Description
Flags	• **u**—Route is up. • **h**—Route is to a host. • **g**—Route is to a gateway. • **e**—Firewall selected this route using Equal Cost Multipath (ECMP). • *—Route is the preferred path to a destination network.
Interface	Egress interface the virtual router will use to reach the next hop.
MTU	Maximum transmission unit (MTU); maximum number of bytes that the firewall will transmit in a single TCP packet to this destination.
Refresh	Click to refresh the runtime stats in the table.
Static Route Monitoring	
Destination	IPv4 address and netmask or IPv6 address and prefix length of a network the virtual router can reach.
Next Hop	IP address of the device at the next hop toward the Destination network. A next hop of 0.0.0.0 indicates the default route.
Metric	Metric for the route. When there is more than one static route to the same destination network, the firewall prefers the route with the lowest metric value.
Weight	Weight for the route.
Flags	• **A?B**—Active and learned via BGP • **A C**—Active and a result of an internal interface (connected) - Destination = network • **A H**—Active and a result of an internal interface (connected) - Destination = Host only • **A R**—Active and learned via RIP • **A S**—Active and static • **S**—Inactive (because this route has a higher metric) and static • **O1**—OSPF external type-1 • **O2**—OSPF external type-2 • **Oi**—OSPF intra-area • **Oo**—OSPF inter-area
Interface	Egress interface of the virtual router that will be used to reach the next hop.
Path Monitoring (Fail On)	If path monitoring is enabled for this static route, Fail On indicates: • **All**—Firewall considers the static route down and will fail over if all of the monitored destinations for the static route are down. • **Any**—Firewall considers the static route down and will fail over if any one of the monitored destinations for the static route is down. If static route path monitoring is disabled, Fail On indicates **Disabled**.

Runtime Stat	Description
Status	Status of the static route based on ICMP pings to the monitored destinations: **Up**, **Down**, or path monitoring for the static route is **Disabled**.
Refresh	Refreshes the runtime stats in the table.

RIP Tab

The following table describes the virtual router's Runtime Stats for RIP.

RIP Runtime Stats	Description
Summary Tab	
Interval Seconds	Number of seconds in an interval. RIP uses this value (a length of time) to control its Update, Expire, and Delete Intervals.
Update Intervals	Number of intervals between RIP route advertisement updates that the virtual router sends to peers.
Expire Intervals	Number of intervals since the last update the virtual router received from a peer, after which the virtual router marks the routes from the peer as unusable.
Delete Intervals	Number of intervals after a route has been marked as unusable that, if no update is received, the firewall deletes the route from the routing table.
Interface Tab	
Address	IP address of an interface on the virtual router where RIP is enabled.
Auth Type	Type of authentication: simple password, MD5, or none.
Send Allowed	Check mark indicates this interface is allowed to send RIP packets.
Receive Allowed	Check mark indicates this interface is allowed to receive RIP packets.
Advertise Default Route	Check mark indicates that RIP will advertise its default route to its peers.
Default Route Metric	Metric (hop count) assigned to the default route. The lower the metric value, the higher priority it has in the route table to be selected as the preferred path.
Key Id	Authentication key used with peers.
Preferred	Preferred key for authentication.
Peer Tab	
Peer Address	IP address of a peer to the virtual router's RIP interface.

RIP Runtime Stats	Description
Last Update	Date and time that the last update was received from this peer.
RIP Version	RIP version the peer is running.
Invalid Packets	Count of invalid packets received from this peer. Possible causes that the firewall cannot parse the RIP packet: x bytes over a route boundary, too many routes in packet, bad subnet, illegal address, authentication failed, or not enough memory.
Invalid Routes	Count of invalid routes received from this peer. Possible causes: route is invalid, import fails, or not enough memory.

BGP Tab

The following table describes the virtual router's Runtime Stats for BGP.

BGP Runtime Stats	Description
Summary Tab	
Router Id	Router ID assigned to the BGP instance.
Reject Default Route	Indicates whether the Reject Default Route option is configured, which causes the VR to ignore any default routes that are advertised by BGP peers.
Redistribute Default Route	Indicates whether the Allow Redistribute Default Route option is configured.
Install Route	Indicates whether the Install Route option is configured, which causes the VR to install BGP routes in the global routing table.
Graceful Restart	Indicates whether or not Graceful Restart is enabled (support).
AS Size	Indicates whether the AS Format size selected is 2 Byte or 4 Byte.
Local AS	Number of the AS to which the VR belongs.
Local Member AS	Local Member AS number (valid only if the VR is in a confederation). The field is 0 if the VR is not in a confederation.
Cluster ID	Displays the Reflector Cluster ID configured.
Default Local Preference	Displays the Default Local Preference configured for the VR.
Always Compare MED	Indicates whether the Always Compare MED option is configured, which enables a comparison to choose between routes from neighbors in different autonomous systems.
Aggregate Regardless MED	Indicates whether the Aggregate MED option is configured, which enables route aggregation even when routes have different MED values.

BGP Runtime Stats	Description
Deterministic MED Processing	Indicates whether the Deterministic MED comparison option is configured, which enables a comparison to choose between routes that are advertised by IBGP peers (BGP peers in the same AS).
Current RIB Out Entries	Number of entries in the RIB Out table.
Peak RIB Out Entries	Peak number of Adj-RIB-Out routes that have been allocated at any one time.
Peer Tab	
Name	Name of the peer.
Group	Name of the peer group to which this peer belongs.
Local IP	IP address of the BGP interface on the VR.
Peer IP	IP address of the peer.
Peer AS	Autonomous system to which the peer belongs.
Password Set	Yes or no indicates whether authentication is set.
Status	Status of the peer, such as Active, Connect, Established, Idle, OpenConfirm, or OpenSent.
Status Duration (secs.)	Duration of the peer's status.
Peer Group Tab	
Group Name	Name of a peer group.
Type	Type of peer group configured, such as EBGP or IBGP.
Aggregate Confed. AS	Yes or no indicates whether the Aggregate Confederation AS option is configured.
Soft Reset Support	Yes or no indicates whether the peer group supports soft reset. When routing policies to a BGP peer change, routing table updates might be affected. A soft reset of BGP sessions is preferred over a hard reset because a soft reset allows routing tables to be updated without clearing the BGP sessions.
Next Hop Self	Yes or no indicates whether this option is configured.
Next Hop Third Party	Yes or no indicates whether this option is configured.
Remove Private AS	Indicates whether updates will have private AS numbers removed from the AS_PATH attribute before the update is sent.

BGP Runtime Stats	Description
Local RIB Tab	
Prefix	Network prefix and subnet mask in the Local Routing Information Base.
Flag	* indicates the route was chosen as the best BGP route.
Next Hop	IP address of the next hop toward the Prefix.
Peer	Name of peer.
Weight	Weight attribute assigned to the Prefix. If the firewall has more than one route to the same Prefix, the route with the highest weight is installed in the IP routing table.
Local Pref.	Local preference attribute for the route, which is used to choose the exit point toward the prefix if there are multiple exit points. A higher local preference is preferred over a lower local preference.
AS Path	List of autonomous systems in the path to the Prefix network; the list is advertised in BGP updates.
Origin	Origin attribute for the Prefix; how BGP learned of the route.
MED	Multi-Exit Discriminator (MED) attribute of the route. The MED is a metric attribute for a route, which the AS advertising the route suggests to an external AS. A lower MED is preferred over a higher MED.
Flap Count	Number of flaps for the route.
RIB Out Tab	
Prefix	Network routing entry in the Routing Information Base.
Next Hop	IP address of the next hop toward the Prefix.
Peer	Peer to which the VR will advertise this route.
Local Pref.	Local preference attribute to access the prefix, which is used to choose the exit point toward the prefix if there are multiple exit points. A higher local preference is preferred over a lower local preference.
AS Path	List of autonomous systems in the path to the Prefix network.
Origin	Origin attribute for the Prefix; how BGP learned of the route.
MED	Multi-Exit Discriminator (MED) attribute to the Prefix. The MED is a metric attribute for a route, which the AS that is advertising the route suggests to an external AS. A lower MED is preferred over a higher MED.
Adv. Status	Advertised status of the route.

BGP Runtime Stats	Description
Aggr. Status	Indicates whether this route is aggregated with other routes.

Multicast Tab

The following table describes the virtual router's Runtime Stats for IP multicast.

Multicast Runtime Stats	Description
FIB Tab	
Group	Route entry in the forwarding information base (FIB); multicast group address to which the virtual router will forward packets.
Source	Source address of multicast packets for the group.
Incoming Interfaces	Interfaces where multicast packets for the group arrive.
Outgoing Interfaces	Interfaces out which the virtual router forwards multicast packets for the group.
IGMP Interface Tab	
Interface	Interface that has IGMP enabled.
Version	Version 1, 2, or 3 of Internet Group Management Protocol (IGMP) running on the virtual router.
Querier	IP address of the IGMP querier on the multiaccess segment connected to the interface.
Querier Up Time	Number of seconds that the IGMP querier has been up.
Querier Expiry Time	Number of seconds remaining before the Other Querier Present timer expires.
Robustness	Robustness variable of the IGMP interface.
Groups Limit	Maximum number of groups per interface that IGMP can process simultaneously.
Sources Limit	Maximum number of sources per interface that IGMP can process simultaneously.
Immediate Leave	Yes or no indicates whether Immediate Leave is configured. Immediate leave indicates that the virtual router will remove an interface from the forwarding table entry without sending the interface IGMP group-specific queries.
IGMP Membership Tab	
Interface	Name of the interface that belongs to the group.

Multicast Runtime Stats	Description
Group	Address of the multicast group to which the interface belongs.
Source	IP address of the source sending multicast packets to the group.
Up Time	Number of seconds this membership has been up.
Expiry Time	Number of seconds remaining before membership expires.
Filter Mode	Include or exclude the source. The virtual router is configured to include all traffic, or only traffic from this source (include), or traffic from any source except this one (exclude).
Exclude Expiry	Number of seconds remaining before the interface Exclude state expires.
V1 Host Timer	Time remaining until the local router assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to the interface.
V2 Host Timer	Time remaining until the local router assumes that there are no longer any IGMP Version 2 members on the IP subnet attached to the interface.
PIM Group Mapping Tab	
Group	IP address of the group mapped to a Rendezvous Point.
RP	IP address of Rendezvous Point for the group.
Origin	Indicates where the virtual router learned of the RP.
PIM Mode	ASM or SSM.
Inactive	Indicates whether the mapping of the group to the RP is inactive.
PIM Interface Tab	
Interface	Name of interface participating in PIM.
Address	IP address of the interface.
DR	IP address of the Designated Router on the multiaccess segment connected to the interface.
Hello Interval	Hello interval configured (in seconds).
Join/Prune Interval	Interval configured for Join and Prune messages (in seconds).
Assert Interval	PIM Assert interval configured (in seconds) for the virtual router to send Assert messages. PIM uses the Assert mechanism to initiate the election of the PIM forwarder for the multiaccess network.

Multicast Runtime Stats	Description
DR Priority	Priority configured for the Designated Router on the multiaccess segment connected to the interface.
BSR Border	Yes or no indicates whether the interface is on a virtual router that is a bootstrap router (BSR) located at the border of an enterprise LAN.
PIM Neighbor Tab	
Interface	Name of interface in the virtual router.
Address	IP address of the PIM neighbor reachable from the interface.
Secondary Address	Secondary IP address of the PIM neighbor reachable from the interface.
Up Time	Length of time the neighbor has been up.
Expiry Time	Length of time remaining before the neighbor expires because the virtual router is not receiving hello packets from the neighbor.
Generation ID	Randomly generated 32-bit value that is regenerated every time PIM forwarding is started or restarted on the interface (includes when the router itself restarts).
DR Priority	Designated Router priority that the virtual router received in the last PIM hello message from this neighbor.

BFD Summary Information Tab

BFD summary information includes the following data.

BFD Summary Information Runtime Stats	Description
Interface	Interface that is running BFD.
Protocol	Static route (IP address family of static route) or dynamic routing protocol that is running BFD on the interface.
Local IP Address	IP address of the interface where you configured BFD.
Neighbor IP Address	IP address of BFD neighbor.
State	BFD states of the local and remote BFD peers: **admin down**, **down**, **init**, or **up**.
Uptime	Length of time BFD has been up (hours, minutes, seconds, and milliseconds).
Discriminator (local)	Discriminator for local BFD peer. A discriminator is a unique, nonzero value the peers use to distinguish multiple BFD sessions between them.

BFD Summary Information Runtime Stats	Description
Discriminator (remote)	Discriminator for remote BFD peer.
Errors	Number of BFD errors.
Session Details	Click **Details** to see BFD information for a session such as the IP addresses of the local and remote neighbors, the last received remote diagnostic code, number of transmitted and received control packets, number of errors, information about the last packet causing state change, and more.

More Runtime Stats for a Logical Router

After you configure static routes or routing protocols for a logical router, select **Network** > **Logical Routers**, and select **More Runtime Stats** in the last column to see detailed information about the logical router, such as the route table, forwarding table, and the routing protocols and static routes you configured. These windows provide more information than can fit on a single screen for the logical router. The window displays the following tabs:

- Routing (Stats for a Logical Router)
- BGP (Stats for a Logical Router

Routing Stats for a Logical Router

The following table describes the logical router's runtime stats for the Route Table, Forwarding Table, and Static Route Monitoring table.

Runtime Stat	Description
Route Table	
Display Address Family	Select **IPv4 Only**, **IPv6 Only**, or **IPv4 and IPv6** (default) to control which group of addresses to display in the table.
Destination	IPv4 address and netmask or IPv6 address and prefix length of networks the logical router can reach.
Next Hop	IP address of the device at the next hop toward the Destination network. A next hop of 0.0.0.0 indicates the default route.
Protocol	Indicates the route is a static or connected route or learned through BGP.
Metric	Metric for the route. When a routing protocol has more than one route to the same destination network, it prefers the route with the lowest metric value. Each routing protocol uses a different type of metric; for example, RIP uses hop count.

Runtime Stat	Description
Selected	Field is true if enabled; blank if disabled.
Age	Age of the route entry in the routing table.
Active	Field is true if enabled; blank if disabled.
Interface	Egress interface of the logical router that will be used to reach the next hop.
Refresh	Click to refresh the runtime states in the table.
Forwarding Table  *The firewall chooses the best route—from the route table (RIB) toward a destination network—to place in the FIB.*	
Destination	Best IPv4 address and netmask or IPv6 address and prefix length to a network the logical router can reach, selected from the Route Table.
Next Hop	IP address of the device at the next hop toward the Destination network. A next hop of 0.0.0.0 indicates the default route.
MTU	Maximum transmission unit (MTU); maximum number of bytes that the firewall will transmit in a single TCP packet to this destination.
Flags	• **u**—Route is up. • **h**—Route is to a host. • **g**—Route is to a gateway. • **e**—Firewall selected this route using Equal Cost Multipath (ECMP). • *—Route is the preferred path to a destination network.
Interface	Egress interface the logical router will use to reach the next hop.
Static Route Monitoring	
Destination	IPv4 address and netmask or IPv6 address and prefix length of a network the logical router can reach.
Next Hop	IP address of the device at the next hop toward the Destination network. A next hop of 0.0.0.0 indicates the default route.
Metric	Metric for the route. When there is more than one static route to the same destination network, the firewall prefers the route with the lowest metric value.

Runtime Stat	Description
Interface	Egress interface of the logical router that will be used to reach the next hop.
Path Monitoring (Fail On)	If path monitoring is enabled for this static route, Fail On indicates: • **All**—Firewall considers the static route down and will fail over if all of the monitored destinations for the static route are down. • **Any**—Firewall considers the static route down and will fail over if any one of the monitored destinations for the static route is down. If static route path monitoring is disabled, Fail On indicates **Disabled**.
Status	Status of the static route based on ICMP pings to the monitored destinations: **Up**, **Down**, or path monitoring for the static route is **Disabled**.
Refresh	Refreshes the runtime stats in the table.

BGP Stats for a Logical Router

The following table describes the logical router's Runtime Stats for BGP.

BGP Runtime Stats	Description
Summary Tab	
Enabled	BGP enabled: yes or no.
Router ID	Router ID of the logical router.
Local AS	AS to which the logical router belongs.
Enforce First AS	Field is true if enabled, blank if not enabled.
Fast External Failover	Field is true if enabled, blank if not enabled.
Default Local Preference	Default local preference configured.
Graceful Restart	Field is true if enabled, blank if not enabled.
Max Peer Restart Time (sec)	Number of seconds configured for Graceful Restart max peer restart time.
Stale Route Time (sec)	Number of seconds configured for Graceful Restart stale route time.

BGP Runtime Stats	Description
Always Compare MED	Field is true if enabled, blank if not enabled.
Deterministic MED Comparison	Field is true if enabled, blank if not enabled.
Peer Tab	
Name	Name of the peer.
Peer Group	Name of the peer group to which this peer belongs.
Local IP	IP address of the BGP interface on the logical router.
Local AS	AS to which the local BGP firewall belongs.
Peer IP	IP address of the peer.
Remote AS	AS to which the peer belongs.
Up/Down	Peer is Up or Down.
State	Established
Peer Group Tab	
Name	Name of a peer group.
Type	Type of peer group configured, such as ebgp or ibgp.
Keep Alive (sec)	Keepalive time in seconds.
Hold Time (sec)	Hold time in seconds.
IP	Field is true if enabled, blank if not enabled.
IPv6	Field is true if enabled, blank if not enabled.
Min. Route Interval (sec)	Minimum route interval in seconds.
Unicast	Field is true if enabled, blank if not enabled.
Route	
Name	IPv4 or IPv6 route in the routing table: an IPv4 or IPv6 address and prefix length.
AS Path	Next AS in the path.
Best Path	Field is true if enabled, blank if not enabled.
MED	0 or blank

BGP Runtime Stats	Description
Metric	0 or blank
Network	
Next Hop	IP address of the next hop to reach the network identified as the route (Name).
Origin	Origin of the route: IGP or incomplete
Path	Next AS in the path.
Path From	Indicates external.
Peer Name	
Prefix	
Prefix Length	
Valid	Field is true if enabled, blank if not enabled.
Weight	Weight for the route.

Network > Routing > Logical Routers

The firewall requires a logical router to obtain routes to other subnets either using static routes that you manually define, or through participation in Layer 3 routing protocols (dynamic routes). Each Layer 3 interface, loopback interface, and VLAN interface defined on the firewall must be associated with a logical router. Each interface can belong to only one logical router.

The logical router is available after you enable **Advanced Routing** in the General Settings of **Device** > **Setup** > **Management** and then commit and reboot the firewall.

The Advanced Route Engine is currently in preview mode only and provides a limited feature set.

Defining a logical router requires that you add Layer 3 interfaces to the logical router and configure any combination of static routes and BGP routing, as required by your network. You can also configure other features, such as ECMP.

What are you looking for?	See
Required elements of a logical router	General Settings of a Logical Router
Configure:	Static Routes BGP BGP Routing Profiles ECMP
View information about a logical router.	More Runtime Stats for a Logical Router

General Settings of a Logical Router

- Network > Routing > Logical Routers > General

When you enable Advanced Routing (**Device** > **Setup** > **Management**), the firewall uses a logical router for static and dynamic routing. A logical router requires that you assign a name and Layer 3 interfaces as described in the following table. The Advanced Routing route engine on the firewall supports only one logical router.

You can optionally configure Equal Cost Multiple Path (ECMP) for the logical router. ECMP processing is a networking feature that enables the firewall to use up to four equal-cost routes to the same destination. Without this feature, if there are multiple equal-cost routes to the same destination, the virtual router chooses one of those routes from the routing table and adds it to its forwarding table; it will not use any of the other routes unless there is an outage in the chosen route. Enabling ECMP functionality on a virtual router allows the firewall have up to four equal-cost paths to a destination in its forwarding table, allowing the firewall to:

- Load balance flows (sessions) to the same destination over multiple equal-cost links.
- Make use of the available bandwidth on all links to the same destination rather than leave some links unused.
- Dynamically shift traffic to another ECMP member to the same destination if a link fails, rather than waiting for the routing protocol or RIB table to elect an alternative path, which can help reduce down time when links fail.

ECMP load balancing is done at the session level, not at the packet level. This means the firewall chooses an equal-cost path at the start of a new session, not each time the firewall receives a packet.

Logical Router General Settings	Description
Name	Specify a name to describe the logical router (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Interface	Add the Layer 3 interfaces that you want to include in the logical router. These interfaces can be used as outgoing interfaces in the logical router's routing table. To specify the interface type, refer to Network > Interfaces. When you add an interface, its connected routes are added automatically.
ECMP	
Enable	Enables Equal-Cost Multiple Path (ECMP) for the logical router.
Symmetric Return	(Optional) Select **Symmetric Return** to cause return packets to egress out the same interface on which the associated ingress packets arrived. That is, the firewall will use the ingress interface on which to send return packets, rather than use the ECMP interface, so the **Symmetric Return** setting overrides load balancing. This behavior occurs only for traffic flows from the server to the client.
Strict Source Path	By default, IKE and IPSec traffic originating at the firewall egresses an interface that the ECMP load-balancing method determines. Select **Strict Source Path** to ensure that IKE and IPSec traffic originating at the firewall always egresses the physical interface to which the source IP address of the IPSec tunnel belongs. You would enable Strict Source Path when the firewall has more than one ISP providing equal-cost paths to the same destination. The ISPs typically perform a Reverse Path Forwarding (RPF) check (or a different check to prevent IP address spoofing) to confirm that the traffic is egressing the same interface on which it arrived. Because ECMP by default would choose an egress interface based on the configured ECMP method (instead of choosing the source interface as the egress interface), that would not be what the ISP expects and the ISP could block legitimate return traffic. In this use case, enable Strict Source Path so that the firewall uses the egress interface that is the interface to which the source IP address of the IPSec tunnel belongs.
Max Path	Select the maximum number of equal-cost paths: (2, 3, or 4) to a destination network that can be copied from the RIB to the FIB. Default is 2.
Load-Balancing Method	Choose one of the following ECMP load-balancing algorithms to use on the virtual router. ECMP load balancing is done at the session level, not at the packet level. This means that the firewall (ECMP) chooses an

Logical Router General Settings	Description
	equal-cost path at the start of a new session, not each time a packet is received. • **IP Modulo**—By default, the virtual router load balances sessions using this option, which uses a hash of the source and destination IP addresses in the packet header to determine which ECMP route to use. • **IP Hash**—There are two IP hash methods that determine which ECMP route to use: • If you select **IP Hash**, by default the firewall uses a hash of the source and destination IP addresses. • Alternatively, you can select **Use Source Address Only** (available in PAN-OS 8.0.3 and later releases). This IP hash method ensures that all sessions belonging to the same source IP address always take the same path. • Optionally select **Use Source/Destination Ports** to include the ports in either hash calculation. You can also enter a **Hash Seed** value (an integer) to further randomize load balancing. • **Weighted Round Robin**—This algorithm can be used to take into consideration different link capacities and speeds. Upon choosing this algorithm, the Interface window opens. Click **Add** and select an **Interface** to be included in the weighted round robin group. For each interface, enter the **Weight** to be used for that interface. **Weight** defaults to 100; range is 1-255. The higher the weight for a specific equal-cost path, the more often that equal-cost path will be selected for a new session. A higher speed link should be given a higher weight than a slower link, so that more of the ECMP traffic goes over the faster link. Click **Add** again to add another interface and weight. • **Balanced Round Robin**—Distributes incoming ECMP sessions equally across links.

Static Routes for a Logical Router

- Network > Routing > Logical Routers > Static

Optionally add one or more static routes. Select **IP** or **IPv6** and **Add** the route using an IPv4 or IPv6 address. It is usually necessary to configure default routes (0.0.0.0/0) here. Default routes are applied for destinations that are not found in the logical router's routing table.

Static Route Settings	Description
Name	Enter a name to identify the static route (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Destination	Enter an IP address and network mask in Classless Inter-domain Routing (CIDR) notation: *ip_address/mask* (for example, 192.168.2.0/24 for IPv4 or 2001:db8::/32 for IPv6). Alternatively, you can create an address object of type IP Netmask.

Static Route Settings	Description
Interface	Select the outgoing interface to forward packets to the destination, or configure the next hop settings, or both. Specify an interface for stricter control over which interface the firewall uses rather than using the interface in the route table for the next hop of this route.
Next Hop	Select one of the following: • **IP Address**—Select to enter the IP address of the next hop router, or select or create an address object of type IP Netmask. The address object must have a netmask of /32 for IPv4, or /128 for IPv6. You must **Enable IPv6 on the interface** (when you configure Layer 3 interfaces) to use an IPv6 next hop address. • **Discard**—Select if you want to drop traffic that is addressed to this destination. • **None**—Select if there is no next hop for the route. For example, a point-to-point connect does not require a next hop because there is only one way for packets to go.
Admin Distance	Specify the administrative distance for the static route (range is 10 to 240; default is 10).
Metric	Specify a valid metric for the static route (range is 1 to 65,535; default is 10).
Path Monitoring	Select and enable path monitoring for the static route.
Failure Condition	Select the condition under which the firewall considers the monitored path down and thus the static route down: • **Any**—If any one of the monitored destinations for the static route is unreachable by ICMP, the firewall removes the static route from the RIB and FIB and adds the dynamic or static route that has the next lowest metric going to the same destination to the FIB. • **All**—If all of the monitored destinations for the static route are unreachable by ICMP, the firewall removes the static route from the RIB and FIB and adds the dynamic or static route that has the next lowest metric going to the same destination to the FIB. Select **All** to avoid the possibility of a single monitored destination signaling a static route failure when that monitored destination is simply offline for maintenance, for example.
Preemptive Hold Time (min)	Enter the number of minutes a downed path monitor must remain in Up state—the path monitor evaluates all of its member monitored destinations and must remain Up before the firewall reinstalls the static route into the RIB. If the timer expires without the link going down or flapping, the link is deemed stable, path monitor can remain Up, and the firewall can add the static route back into the RIB. If the link goes down or flaps during the hold time, path monitor fails and the timer restarts when the downed monitor returns to Up state. A **Preemptive Hold Time** of zero causes the firewall to reinstall the static

Static Route Settings	Description
	route into the RIB immediately upon the path monitor coming up. Range is 0 to 1,440; default is 2.
Name	Enter a name for the monitored destination (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Enable	Select to enable path monitoring of this specific destination for the static route; the firewall sends ICMP pings to this destination.
Source IP	Select the IP address that the firewall will use as the source in the ICMP ping to the monitored destination: • If the interface has multiple IP addresses, select one. • If you select an interface, the firewall uses the first IP address assigned to the interface by default. • If you select **DHCP (Use DHCP Client address)**, the firewall uses the address that DHCP assigned to the interface. To see the DHCP address, select **Network** > **Interfaces** > **Ethernet** and in the row for the Ethernet interface, click on **Dynamic DHCP Client**. The IP Address appears in the Dynamic IP Interface Status window.
Destination IP	Enter a robust, stable IP address or address object for which the firewall will monitor the path. The monitored destination and the static route destination must use the same address family (IPv4 or IPv6)
Ping Interval (sec)	Specify the ICMP ping interval in seconds to determine how frequently the firewall monitors the path (pings the monitored destination; range is 1 to 60; default is 3).
Ping Count	Specify the number of consecutive ICMP ping packets that do not return from the monitored destination before the firewall considers the link down. Based on the **Any** or **All** failure condition, if path monitoring is in failed state, the firewall removes the static route from the RIB (range is 3 to 10; default is 5). For example, a Ping Interval of 3 seconds and Ping Count of 5 missed pings (the firewall receives no ping in the last 15 seconds) means path monitoring detects a link failure. If path monitoring is in failed state and the firewall receives a ping after 15 seconds, the link is deemed up; based on the **Any** or **All** failure condition, path monitoring to **Any** or **All** monitored destinations can be deemed up, and the Preemptive Hold Time starts.

BGP Routing for a Logical Router

- Network > Routing> Logical Routers > BGP

The table describes the settings to configure BGP, peer groups, peers, and redistribution for a logical router.

BGP Settings	Description
General	
Enable	Enable BGP for the logical router.
Router ID	Assign a Router ID to BGP for the logical router, which is typically an IPv4 address to ensure the Router ID is unique.
Local AS	Assign the local autonomous system (AS) to which the logical router belongs based on the Router ID (range for a 2-byte or 4-byte AS number is to 1 to 4,294,967,295).
ECMP Multiple AS Support	Enable if you configured ECMP and you want to run ECMP over multiple BGP autonomous systems.
Enforce First AS	Select to cause the firewall to drop an incoming Update message from an EBGP peer that does not list the EBGP peer's own AS number as the first AS number in the AS_PATH attribute. (Enabled by default.)
Fast Failover	Fast failover of EBGP is enabled by default. Disable EBGP fast failover if it causes the firewall to unnecessarily withdraw BGP routes.
Default Local Preference	Specify the default local preference that can be used to determine preferences among different paths; range is 0 to 4,294,967,295; default is 100.
Graceful Restart—Enable	Enables graceful restart for BGP so that packet forwarding is not disrupted during a BGP restart (enabled by default).
Stale Route Time	Specify the length of time, in seconds, that a route can stay in the stale state (range is 1 to 3,600; default is 120).
Max Peer Restart Time	Specify the maximum length of time, in seconds, that the local device accepts as a grace period restart time for peer devices (range is 1 to 3,600; default is 120).
Path Selection—Always Compare MED	Select to choose paths from neighbors in different autonomous systems; default is disabled. The Multi-Exit Discriminator (MED) is an external metric that lets neighbors know about the preferred path into an AS. A lower value is preferred over a higher value.
Deterministic MED Comparison	Select to choose between routes that are advertised by IBGP peers (BGP peers in the same AS). Default is enabled.
Peer Group	
Name	Enter a name for the BGP peer group.
Enable	Enable the peer group.
Type	Select the type of peer group as **IBGP** (Internal BGP, peering within an AS) or **EBGP** (External BGP—peering between two autonomous systems).

BGP Settings	Description
AFI IP Unicast	Select or create an AFI IPv4 profile to apply the settings in the profile to the peer group; default is **None**.
AFI IPv6 Unicast	Select or create an AFI IPv6 profile to apply the settings in the profile to the peer group; default is **None**.
Auth Profile	Select or create an authentication profile to authenticate BGP peer communications; default is **None**.
Timer Profile	Select or create a Timers profile to apply to the peer group; default is **None**.
Multi Hop	Set the time-to-live (TTL) value in the IP header. Range is 1 to 255; a setting of 0 means use the default value: 1 for EBGP; 255 for IBGP.
Peer	
Name	Enter a name for the BGP peer.
Enable	Enable the BGP peer.
Peer AS	Enter the AS to which the peer belongs; range is 1 to 4,294,967,295.
Peer—Addressing	
Inherit AFI/SAFI config from peer-group	Select for the peer to inherit the AFI and Subsequent AFI (SAFI) from the peer group.
AFI IP Unicast	(Available if **Inherit AFI/SAFI config from peer** is disabled) Select or create an AFI IPv4 profile to apply the settings in the profile to the peer; default is **None**.
AFI IPv6 Unicast	(Available if **Inherit AFI/SAFI config from peer** is disabled) Select or create an AFI IPv6 profile to apply the settings in the profile to the peer; default is **None**.
Local Address - Interface	Select the Layer 3 interface for which you are configuring BGP. Interfaces configured with a static IP address and interfaces configured as a DHCP client are available to select. If you select an interface where DHCP assigns the address, the **IP** address will indicate **None**. DHCP will later assign an IP address to the interface; you can see the address when you view **More Runtime Stats** for the logical router.
IP	If the interface has more than one IP address, enter the IP address and netmask you want to use.
Peer Address - IP	Enter the IP address of the peer.
Peer—Connection Options These settings override the same option you have set for the peer group to which the peer belongs.	

BGP Settings	Description
Auth Profile	Select or create an Authentication profile. Alternatively, select **inherit (Inherit from Peer-Group)** or **None**, both of which cause the peer to use the Auth profile specified for the peer group.
Timer Profile	Select or create a Timers profile. Alternatively, select **inherit (Inherit from Peer-Group)** or **None**, both of which cause the peer to use the Timers profile specified for the peer group.
Multi Hop	Select **inherit (Inherit from Peer-Group)** or **None**, both of which cause the peer to use the value specified for the peer group.
Peer—Advanced	
Enable Sender Side Loop Detection	Select to cause the firewall to check the AS_PATH attribute of a route in its forwarding information base (FIB) before it sends the route in an Update, to ensure that the peer AS number is not on the AS_PATH list. If it is, the firewall removes it to prevent a loop. Default is enabled.
BGP Redistribution	
Redistribution Rules	
IPv4 Unicast	Select or create a Redistribution profile to specify which static or connected IPv4 routes to redistribute to the IPv4 unicast route table. Default is **None**.
IPv6 Unicast	Select or create a Redistribution profile to specify which static or connected IPv6 routes to redistribute to the IPv6 unicast route table. Default is **None**.
Network	
IPv4 or IPv6	Select **IPv4** or **IPv6**.
Network	Add a corresponding IPv4 or IPv6 network address; subnets with matching network addresses are advertised to BGP peers of the logical router.
Unicast	Select to install the matching routes into the Unicast routing table of all BGP peers.

Network > Routing > Routing Profiles > BGP

For a logical router, use BGP profiles to efficiently apply configuration to BGP peer groups, peers, or redistribution rules. For example, you can apply a Timer Profile or Authentication Profile to a BGP peer group or a peer. You can apply an Address Family (AFI) profile for IPv4 and for IPv6 to a peer group. You can apply a Redistribution profile for IPv4 and for IPv6 to BGP redistribution.

BGP Routing Profiles	Description
BGP Auth Profile	

BGP Routing Profiles	Description
Name	Enter a name for the Authentication profile (maximum of 31 characters).
Secret	Enter the Secret and **Confirm Secret**. The Secret is used as a key in MD5 authentication.
BGP Timers Profile	
Name	Enter a name for the Timers profile (maximum of 31 characters).
Keep Alive Interval (sec)	Enter the interval, in seconds, after which routes from the peer are suppressed according to the Hold Time setting (range is 0 to 1,200; default is 30).
Hold Time (sec)	Enter the length of time, in seconds, that may elapse between successive Keepalive or Update messages from the peer before the peer connection is closed (range is 3 to 3,600; default is 90).
Minimum Route Advertise Interval (sec)	Enter the minimum about of time, in seconds, that must occur between two successive Update messages (that a BGP speaker [the firewall] sends to a BGP peer) that advertise routes or withdrawal of routes (range is 1 to 600; default is 30).
BGP Address Family Profile	
Name	Enter a name for the Address Family Identifier (AFI) profile (maximum of 31 characters).
IPv4 or IPv6	Select the type of AFI profile (IPv4 or IPv6).
Advertise all paths to a peer	Advertise all routes in the BGP routing information base (RIB).
Advertise the best path per neighboring AS	Enable to ensure that BGP advertises the best path for each neighboring AS, and not a generic path for all autonomous systems. Disable this if you want to advertise the same path to all autonomous systems.
Allow AS in	Specify whether to allow routes that include the firewall's own autonomous system (AS) number: • **Origin**—Accept routes even if the firewall's own AS is present in the AS_PATH. • **Occurrence**—Number of times the firewall's own AS can be in an AS_PATH. • **None**—(default setting) No action taken.
Override ASNs in outbound updates if AS-Path equals Remote-AS	You might use the BGP AS override feature if you have multiple sites belonging to the same AS (AS 64512, for example) and there is another AS between them. A router between the two sites receives an Update advertising a route that can access AS 64512. To avoid the second site dropping the Update because it is also in AS 64512, the intermediate router replaces AS 64512 with its own ASN, AS 64522, for example.

BGP Routing Profiles	Description
Originate Default Route	Select to advertise a default route. Disable if you want to advertise only routes that go to specific destinations.
Num_prefixes	Enter the maximum number of prefixes to accept from peer.
Threshold (%)	Enter the threshold percentage of the maximum number of prefixes. If the peer advertises more than the threshold, the firewall takes the specified Action (warning or restart). Range is 1 to 100%.
Action	Specify the action the firewall takes on the BGP connection after the maximum number of prefixes is exceeded: **Warning Only** message in logs or **Restart** the BGP peer connection.
Next Hop	Select the next hop: • **None**—No action; calculate the next hop for this neighbor. • **Self**—Disable next-hop calculation and advertise routes with local next-hop. • **Self Force**—Force set the next hop to self for the reflected routes.
Remove Private AS	To have BGP remove private AS numbers form the AS_PATH attribute in Updates that the firewall sends to a peer in another AS, select one of the following: • **All**—Remove all private AS numbers. • **Replace AS**—Replace all private AS numbers with the firewall's AS number. • **None**—(default setting) No action taken.
Route Reflector Client	Enable the firewall as a BGP Route Reflector Client.
Send Community	Select the type of BGP community attribute to send in outbound Update messages: • **All**—Send all communities. • **Both**—Send standard and extended communities. • **Extended**—Send extended communities. • **Large**—Send large communities. • **Standard**—Send standard communities. • **None**—Do not send any communities.
BGP Redistribution Profile	
Name	Enter a name for the Redistribution profile (maximum of 31 characters).
IPv4 or IPv6	Select IPv4 or IPv6 Address Family Identifier (AFI) to specify which type of route is redistributed.
Static	Select **Static** and **Enable** to redistribute IPv4 or IPv6 static routes (that match the AFI you selected) into the BGP routing information base (RIB) of the BGP peers.

BGP Routing Profiles	Description
Metric	Enter the metric to apply to the static routes being redistributed into BGP (range is 1 to 65,535).
Connected	Select **Connected** and **Enable** to redistribute IPv4 or IPv6 connected routes (that match the AFI you selected) into the BGP routing information base (RIB) of the BGP peers.
Metric	Enter the metric to apply to the connected routes being redistributed into BGP (range is 1 to 65,535).

Network > IPSec Tunnels

Select **Network** > **IPSec Tunnels** to establish and manage IPSec VPN tunnels between firewalls. This is the Phase 2 portion of the IKE/IPSec VPN setup.

What are you looking for?	See:
Manage IPSec VPN tunnels.	IPSec VPN Tunnel Management
Configure an IPSec tunnel.	IPSec Tunnel General Tab
	IPSec Tunnel Proxy IDs Tab
View IPSec tunnel status.	IPSec Tunnel Status on the Firewall
Restart or refresh an IPSec tunnel.	IPSec Tunnel Restart or Refresh
Looking for more?	Set up an IPSec tunnel.

IPSec VPN Tunnel Management

- Network > IPSec Tunnels

The following table describes how to manage your IPSec VPN tunnels.

Fields to Manage IPSec VPN Tunnels	
Add	**Add** a new IPSec VPN tunnel. See IPSec Tunnel General Tab for instructions on configuring the new tunnel.
Delete	**Delete** a tunnel that you no longer need.
Enable	**Enable** a tunnel that has been disabled (tunnels are enabled by default).
Disable	**Disable** a tunnel that you don't want to use but are not, yet, ready to delete.
PDF/CSV	Export the IPSec Tunnel configuration in **PDF/CSV** format. You can apply filters to customize the table output and include only the columns you need. Only the columns visible in the Export dialog are exported. See Export Configuration Table Data.

IPSec Tunnel General Tab

- Network > IPSec Tunnels > General

Use the following fields to set up an IPSec tunnel.

IPSec Tunnel General Settings	Description
Name	Enter a **Name** to identify the tunnel (up to 63 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. The 63-character limit for this field includes the tunnel name in addition to the Proxy ID, which is separated by a colon character.
Tunnel Interface	Select an existing tunnel interface, or click **New Tunnel Interface**. For information on creating a tunnel interface, refer to Network > Interfaces > Tunnel.
IPv4 or IPv6	Select **IPv4** or **IPv6** to configure the tunnel to have endpoints with that IP type of address.
Type	Select whether to use an automatically generated or manually entered security key. **Auto key** is recommended.
Auto Key	If you choose **Auto Key**, specify the following: • **IKE Gateway**—Refer to Network > Network Profiles > IKE Gateways for descriptions of the IKE gateway settings. • **IPSec Crypto Profile**—Select an existing profile or keep the default profile. To define a new profile, click **New** and follow the instructions in Network > Network Profiles > IPSec Crypto. • Click **Show Advanced Options** to access the remaining fields. • **Enable Replay Protection**—Select to protect against replay attacks. • **Copy TOS Header**—Copy the (Type of Service) TOS field from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original TOS information. This also copies the Explicit Congestion Notification (ECN) field. • **Add GRE Encapsulation**—Select to add a GRE header encapsulated in the IPSec tunnel. The firewall generates a GRE header after the IPSec header for interoperability with other vendor tunnel endpoints, thus sharing a GRE tunnel with the IPSec tunnel. • **Tunnel Monitor**—Select to alert the device administrator of tunnel failures and to provide automatic failover to another interface.  *You need to assign an IP address to the tunnel interface for monitoring.* • **Destination IP**—Specify an IP address on the other side of the tunnel that the tunnel monitor will use to determine if the tunnel is working properly. • **Profile**—Select an existing profile that will determine the actions that are taken if the tunnel fails. If the action specified in the monitor profile is wait-recover, the firewall will wait for the tunnel to become functional and will NOT seek an alternate path with the route table. If the fail-over action is used, the firewall will check the route table to see if there is an alternate route that can be used to reach the destination. For more information, see Network > Network Profiles > Monitor.
Manual Key	If you choose **Manual Key**, specify the following:

IPSec Tunnel General Settings	Description
	• **Local SPI**—Specify the local security parameter index (SPI) for packet traversal from the local firewall to the peer. SPI is a hexadecimal index that is added to the header for IPSec tunneling to assist in differentiating between IPSec traffic flows. • **Interface**—Select the interface that is the tunnel endpoint. • **Local Address**—Select the IP address for the local interface that is the endpoint of the tunnel. • **Remote SPI**—Specify the remote security parameter index (SPI) for packet traversal from the remote firewall to the peer. • **Protocol**—Choose the protocol for traffic through the tunnel (**ESP** or **AH**). • **Authentication**—Choose the authentication type for tunnel access (**SHA1**, **SHA256**, **SHA384**, **SHA512**, **MD5**, or **None**). • **Key/Confirm Key**—Enter and confirm an authentication key. • **Encryption**—Select an encryption option for tunnel traffic (**3des**, **aes-128-cbc**, **aes-192-cbc**, **aes-256-cbc**, **des**, or **null** [no encryption]). • **Key/Confirm Key**—Enter and confirm an encryption key.
GlobalProtect Satellite	If you choose **GlobalProtect Satellite**, specify the following: • **Name**—Enter a name to identify the tunnel (up to **31** characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. • **Tunnel Interface**—Select an existing tunnel interface, or click New Tunnel Interface. • **Portal Address**—Enter the IP address of the GlobalProtect™ Portal. • **Interface**—Select the interface from the drop-down that is the egress interface to reach the GlobalProtect Portal. • **Local IP Address**—Enter the IP address of the egress interface that connects to the GlobalProtect Portal. • **Advanced Options** • **Publish all static and connected routes to Gateway**—Select to publish all routes from the satellite to the GlobalProtect Gateway in which this satellite is connected. • **Subnet**—Click **Add** to manually add local subnets for the satellite location. If other satellites are using the same subnet information, you must NAT all traffic to the tunnel interface IP. Also, the satellite must not share routes in this case, so all routing will be done through the tunnel IP. • **External Certificate Authority**—Select if you will use an external CA to manage certificates. Once you have your certificates generated, you will need to import them into the satellite and select the **Local Certificate** and the **Certificate Profile**.

IPSec Tunnel Proxy IDs Tab

- Network > IPSec Tunnels > Proxy IDs

The **IPSec Tunnel Proxy IDs** tab is separated into two tabs: **IPv4** and **IPv6**. The help is similar for both types; the differences between IPv4 and IPv6 are described in the **Local** and **Remote** fields in the following table.

The **IPSec Tunnel Proxy IDs** tab is also used for specifying traffic selectors for IKEv2.

Proxy IDs IPv4 and IPv6 Settings	Description
Proxy ID	Click **Add** and enter a name to identify the proxy. For an IKEv2 traffic selector, this field is used as the Name.
Local	For IPv4: Enter an IP address or subnet in the format x.x.x.x/mask (for example, 10.1.2.0/24). For IPv6: Enter an IP address and prefix length in the format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/prefix-length (or per IPv6 convention, for example, 2001:DB8:0::/48). IPv6 addressing does not require that all zeros be written; leading zeros can be omitted and one grouping of consecutive zeros can be replaced by two adjacent colons (::). For an IKEv2 traffic selector, this field is converted to Source IP Address.
Remote	If required by the peer: For IPv4, enter an IP address or subnet in the format x.x.x.x/mask (for example, 10.1.1.0/24). For IPv6, enter an IP address and prefix length in the format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/prefix-length (or per IPv6 convention, for example, 2001:DB8:55::/48). For an IKEv2 traffic selector, this field is converted to Destination IP Address.
Protocol	Specify the protocol and port numbers for the local and remote ports: **Number**—Specify the protocol number (used for interoperability with third-party devices). • **Any**—Allow TCP and/or UDP traffic. • **TCP**—Specify the local and remote TCP port numbers. • **UDP**—Specify the local and remote UDP port numbers. Each configured proxy ID will count towards the IPSec VPN tunnel capacity of the firewall. This field is also used as an IKEv2 traffic selector.

IPSec Tunnel Status on the Firewall

- Network > IPSec Tunnels

To view the status of currently defined IPSec VPN tunnels, open the **IPSec Tunnels** page. The following status information is reported on the page:

- Tunnel Status (first status column)—Green indicates an IPSec phase-2 security association (SA) tunnel. Red indicates that IPSec phase-2 SA is not available or has expired.
- IKE Gateway Status—Green indicates a valid IKE phase-1 SA or IKEv2 IKE SA. Red indicates that IKE phase-1 SA is not available or has expired.
- Tunnel Interface Status—Green indicates that the tunnel interface is up (because tunnel monitor is disabled or because tunnel monitor status is UP and the monitoring IP address is reachable). Red

indicates that the tunnel interface is down because the tunnel monitor is enabled and the remote tunnel monitoring IP address is unreachable.

IPSec Tunnel Restart or Refresh

- Network > IPSec Tunnels

Select **Network** > **IPSec Tunnels** to display status of tunnels. In the first Status column is a link to the tunnel info. Click the tunnel you want to restart or refresh to open the **Tunnel Info** page for that tunnel. Click on one of entries in the list and then click:

- **Restart**—Restart the selected tunnel. A restart disrupts traffic going across the tunnel.
- **Refresh**—Show the current IPSec SA status.

Network > GRE Tunnels

Generic Routing Encapsulation (GRE) tunnel protocol is a carrier protocol that encapsulates a payload protocol. The GRE packet itself is encapsulated in a transport protocol (IPv4 or IPv6). The GRE tunnel connects two endpoints in a point-to-point, logical link between the firewall and a router (or another firewall). Palo Alto Networks firewalls support termination of a GRE tunnel.

What are you looking for?	See:
Building blocks of a GRE tunnel	GRE Tunnels
How to provide interoperability with another vendor's tunnel endpoint	Select **Add GRE Encapsulation** when you create an IPSec tunnel.
Looking for more?	GRE Tunnels

GRE Tunnels

- Network > GRE Tunnels

First configure a tunnel interface (Network > Interfaces > Tunnel). Then add a generic routing encapsulation (GRE) Tunnel and provide the following information, referencing the tunnel interface you created:

GRE Tunnel Fields	Description
Name	Name of the GRE tunnel.
Interface	Select the interface to use as the local GRE tunnel endpoint (source interface), which is an Ethernet interface or subinterface, an Aggregate Ethernet (AE) interface, a loopback interface, or a VLAN interface.
Local Address	Select the local IP address of the interface to use as the tunnel interface address.
Peer Address	Enter the IP address at the opposite end of the GRE tunnel.
Tunnel Interface	Select the Tunnel interface that you configured. (This interface identifies the tunnel when it is the next hop for routing.)
TTL	Enter the TTL for the IP packet encapsulated in the GRE packet (range is 1 to 255; default is 64).
Copy ToS Header	Select to copy the Type of Service (ToS) field from the inner IP header to the outer IP header of the encapsulated packets to preserve the original ToS information.

GRE Tunnel Fields	Description
Keep Alive	Select to enable the Keep Alive function for the GRE tunnel (disabled by default). If you enable Keep Alive, by default it takes three unreturned keepalive packets (Retries) at 10-second intervals for the GRE tunnel to go down, and it takes five Hold Timer intervals at 10-second intervals for the GRE tunnel to come back up.
Interval (sec)	Set the interval between keepalive packets that the local end of the GRE tunnel sends to the tunnel peer, and the interval that each Hold Timer waits after successful keepalive packets before the firewall re-establishes communication with the tunnel peer (range is 1 to 50; default is 10).
Retry	Set the number of intervals that keepalive packets are not returned before the firewall considers the tunnel peer to be down (range is 1 to 255; default is 3).
Hold Timer	Set the number of intervals that keepalive packets are successful before the firewall re-establishes communication with the tunnel peer (range is 1 to 64; default is 5).

Network > DHCP

Dynamic Host Configuration Protocol (DHCP) is a standardized protocol that provides TCP/IP and link-layer configuration parameters and network addresses to dynamically configured hosts on a TCP/IP network. An interface on a Palo Alto Networks firewall can act as a DHCP server, client, or relay agent. Assigning these roles to different interfaces allows the firewall to perform multiple roles.

What are you looking for?	See:
What is DHCP?	DHCP Overview
How does a DHCP server allocate addresses?	DHCP Addressing
Configure an interface on the firewall to act as a:	
	DHCP Server
	DHCP Relay
	Network > DNS Proxy
Looking for more?	DHCP

DHCP Overview

- Network > DHCP

DHCP uses a client-server model of communication. This model consists of three roles that the firewall can fulfill: DHCP client, DHCP server, and DHCP relay agent.

- A firewall acting as a DHCP client (host) can request an IP address and other configuration settings from a DHCP server. Users on client firewalls save configuration time and effort, and need not know the addressing plan of the network or other network resources and options inherited from the DHCP server.
- A firewall acting as a DHCP server can service clients. By using one of the DHCP addressing mechanisms, the administrator saves configuration time and has the benefit of reusing a limited number of IP addresses clients no longer need network connectivity. The server can also deliver IP addressing and DHCP options to multiple clients.
- A firewall acting as a DHCP relay agent listens for broadcast and unicast DHCP messages and relays them between DHCP clients and servers.

DHCP uses User Datagram Protocol (UDP), RFC 768, as its transport protocol. DHCP messages that a client sends to a server are sent to well-known port 67 (UDP—Bootstrap Protocol and DHCP). DHCP messages that a server sends to a client are sent to port 68.

DHCP Addressing

There are three ways that a DHCP server either assigns or sends an IP address to a client:

- **Automatic allocation**—The DHCP server assigns a permanent IP address to a client from its **IP Pools**. On the firewall, a **Lease** specified as **Unlimited** means the allocation is permanent.

- **Dynamic allocation**—The DHCP server assigns a reusable IP address from **IP Pools** of addresses to a client for a maximum period of time, known as a *lease*. This method of address allocation is useful when the customer has a limited number of IP addresses; they can be assigned to clients who need only temporary access to the network.
- **Static allocation**—The network administrator chooses the IP address to assign to the client and the DHCP server sends it to the client. A static DHCP allocation is permanent; it is done by configuring a DHCP server and choosing a **Reserved Address** to correspond to the **MAC Address** of the client firewall. The DHCP assignment remains in place even if the client disconnects (logs off, reboots, has a power outage, etc.).

  Static allocation of an IP address is useful, for example, if you have a printer on a LAN and you do not want its IP address to keep changing, because it is associated with a printer name through DNS. Another example is if a client firewall is used for something crucial and must keep the same IP address, even if the firewall is turned off, unplugged, rebooted, or a power outage occurs.

  Keep the following points in mind when configuring a **Reserved Address**:

  - It is an address from the **IP Pools**. You can configure multiple reserved addresses.
  - If you configure no **Reserved Address**, the clients of the server will receive new DHCP assignments from the pool when their leases expire or if they reboot, etc. (unless you specified that a **Lease** is **Unlimited**).
  - If you allocate every address in the **IP Pools** as a **Reserved Address**, there are no dynamic addresses free to assign to the next DHCP client requesting an address.
  - You may configure a **Reserved Address** without configuring a **MAC Address**. In this case, the DHCP server will not assign the **Reserved Address** to any firewall. You might reserve a few addresses from the pool and statically assign them to a fax and printer, for example, without using DHCP.

DHCP Server

- Network > DHCP > DHCP Server

The following section describes each component of the DHCP server. Before you configure a DHCP server, you should already have configured a Layer 3 Ethernet or Layer 3 VLAN interface that is assigned to a virtual router and a zone. You should also know a valid pool of IP addresses from your network plan that can be designated to be assigned by your DHCP server to clients.

When you add a DHCP server, you configure the settings described in the table below.

DHCP Server Settings	Configured In	Description
Interface	**DHCP Server**	Name of the interface that will serve as the DHCP server.
Mode		Select **enabled** or **auto** mode. **Auto** mode enables the server and disables it if another DHCP server is detected on the network. The **disabled** setting disables the server.
Ping IP when allocating new IP	**DHCP Server** > **Lease**	If you click **Ping IP when allocating new IP**, the server will ping the IP address before it assigns that address to its client. If the ping receives a response, that means a different firewall already has that address, so it is not available for assignment. The server assigns the next address from the pool instead. If you select this option,

DHCP Server Settings	Configured In	Description
		the Probe IP column in the display will have a check mark.
Lease		Specify a lease type. • **Unlimited** causes the server to dynamically choose IP addresses from the IP Pools and assign them permanently to clients. • **Timeout** determines how long the lease will last. Enter the number of **Days** and **Hours**, and optionally, the number of **Minutes**.
IP Pools		Specify the stateful pool of IP addresses from which the DHCP server chooses an address and assigns it to a DHCP client. You can enter a single address, an address/<mask length>, such as 192.168.1.0/24, or a range of addresses, such as 192.168.1.10-192.168.1.20.
Reserved Address		Optionally specify an IP address (format x.x.x.x) from the IP pools that you do not want dynamically assigned by the DHCP server. If you also specify a **MAC Address** (format xx:xx:xx:xx:xx:xx), the **Reserved Address** is assigned to the firewall associated with that MAC address when that firewall requests an IP address through DHCP.
Inheritance Source	**DHCP Server** > **Options**	Select **None** (default) or select a source DHCP client interface or PPPoE client interface to propagate various server settings to the DHCP server. If you specify an **Inheritance Source**, select one or more options below that you want **inherited** from this source. One benefit of specifying an inheritance source is that DHCP options are quickly transferred from the server that is upstream of the source DHCP client. It also keeps the client's options updated if an option on the inheritance source is changed. For example, if the inheritance source firewall replaces its NTP server (which had been identified as the **Primary NTP** server), the client will automatically inherit the new address as its **Primary NTP** server.
Check inheritance source status		If you selected an **Inheritance Source**, click **Check inheritance source status** to open the Dynamic IP Interface Status window, which displays the options that are inherited from the DHCP client.

DHCP Server Settings	Configured In	Description
Gateway	**DHCP Server** > **Options (cont)**	Specify the IP address of the network gateway (an interface on the firewall) that is used to reach any device not on the same LAN as this DHCP server.
Subnet Mask		Specify the network mask that applies to the addresses in the **IP Pools**.
Options		For the following fields, click the drop-down and select **None** or **inherited**, or enter the IP address of the remote server that your DHCP server will send to clients for accessing that service. If you select **inherited**, the DHCP server inherits the values from the source DHCP client specified as the **Inheritance Source**. The DHCP server sends these settings to its clients. • **Primary DNS**, **Secondary DNS**—IP address of the preferred and alternate Domain Name System (DNS) servers. • **Primary WINS**, **Secondary WINS**—IP address of the preferred and alternate Windows Internet Name Service (WINS) servers. • **Primary NIS**, **Secondary NIS**—IP address of the preferred and alternate Network Information Service (NIS) servers. • **Primary NTP**, **Secondary NTP**—IP address of the available network time protocol (NTP) servers. • **POP3 Server**—IP address of a Post Office Protocol version 3 (POP3) server. • **SMTP Server**—IP address of a Simple Mail Transfer Protocol (SMTP) server. • **DNS Suffix**—Suffix for the client to use locally when an unqualified hostname is entered that the client cannot resolve.
Custom DHCP options		Click **Add** and enter the **Name** of the custom option you want the DHCP Server to send to clients. Enter an **Option Code** (range is 1-254). If **Option Code 43** is entered, the Vendor Class Identifier (VCI) field appears. Enter a match criterion that will be compared to the incoming VCI from the client's Option 60. The firewall looks at the incoming VCI from the client's Option 60, finds the matching VCI in its own DHCP server table, and returns the corresponding value to the client in Option 43. The VCI match criterion is a string or hex value. A hex value must have a "0x" prefix. Select **Inherited from DCHP server inheritance source** to have the server inherit the value for that option

DHCP Server Settings	Configured In	Description
		code from the inheritance source instead of you entering an **Option Value**. As an alternative to this option, you can proceed with the following: **Option Type**: Select **IP Address**, **ASCII**, or **Hexadecimal** to specify the type of data used for the Option Value. For **Option Value**, click **Add** and enter the value for the custom option.

DHCP Relay

- Network > DHCP > DHCP Relay

Before configuring a firewall interface as a DHCP relayagent, make sure you have configured a Layer 3 Ethernet or Layer 3 VLAN interface and that you assigned the interface to a virtual router and a zone. You want that interface to be able to pass DHCP messages between clients and servers. Each interface can forward messages to a maximum of eight external IPv4 DHCP servers and eight external IPv6 DHCP servers. A client sends a DHCPDISCOVER message to all configured servers, and the firewall relays the DHCPOFFER message of the first server that responds back to the requesting client.

DHCP Relay Settings	Description
Interface	Name of the interface that will be the DHCP relay agent.
IPv4 / IPv6	Select the type of DHCP server and IP address you will specify.
DHCP Server IP Address	Enter the IP address of the DHCP server to and from which you will relay DHCP messages.
Interface	If you selected IPv6 as the IP address protocol for the DHCP server and specified a multicast address, you must also specify an outgoing interface.

DHCP Client

- Network > Interfaces > Ethernet > IPv4
- Network > Interfaces > VLAN > IPv4

Before configuring a firewall interface as a DHCP client, make sure you have configured a Layer 3 Ethernet or Layer 3 VLAN interface and that you assigned the interface to a virtual router and a zone. Perform this task if you need to use DHCP to request an IPv4 address for an interface on your firewall.

DHCP Client Settings	Description
Type	Select **DHCP Client** and then **Enable** to configure the interface as a DHCP client.

DHCP Client Settings	Description
Automatically create default route pointing to default gateway provided by server	Causes the firewall to create a static route to a default gateway that will be useful when clients are trying to access many destinations that do not need to have routes maintained in a routing table on the firewall.
Default Route Metric	Optionally, enter a **Default Route Metric** (priority level) for the route between the firewall and the DHCP server. A route with a lower number has higher priority during route selection. For example, a route with a metric of 10 is used before a route with a metric of 100 (range is 1-65535; no default).
Show DHCP Client Runtime Info	Displays all settings received from the DHCP server, including DHCP lease status, dynamic IP assignment, subnet mask, gateway, and server settings (DNS, NTP, domain, WINS, NIS, POP3, and SMTP).

Network > DNS Proxy

DNS servers perform the service of resolving a domain name with an IP address and vice versa. When you configure the firewall as a DNS proxy, it acts as an intermediary between clients and servers and as a DNS server by resolving queries from its DNS cache or forwarding queries to other DNS servers. Use this page to configure the settings that determine how the firewall serves as a DNS proxy.

What do you want to know?	See:
How does the firewall proxy DNS requests?	DNS Proxy Overview
How do I configure a DNS proxy?	DNS Proxy Settings
How do I configure static FQDN-to-IP address mappings?	
How can I manage DNS proxies?	Additional DNS Proxy Actions
Looking for more?	DNS

DNS Proxy Overview

You can configure the firewall to act as a DNS server. First, create a DNS proxy and select the interfaces to which the proxy applies. Then specify the default DNS primary and secondary servers to which the firewall sends the DNS queries when it doesn't find the domain name in its DNS proxy cache (and when the domain name doesn't match a proxy rule).

To direct DNS queries to different DNS servers based on domain names, create DNS proxy rules. Specifying multiple DNS servers can ensure localization of DNS queries and increase efficiency. For example, you can forward all corporate DNS queries to a corporate DNS server and forward all other queries to ISP DNS servers.

Use the following tabs to define a DNS proxy (beyond the default DNS primary and secondary servers):

- **Static Entries**—Allows you to configure static FQDN-to-IP address mappings that the firewall caches and sends to hosts in response to DNS queries.
- **DNS Proxy Rules**—Allows you to specify domain names and corresponding primary and secondary DNS servers to resolve queries that match the rule. If the domain name isn't in the DNS proxy cache, the firewall searches for a match in the DNS proxy (on the interface on which the query arrived), and forwards the query to a DNS server based on the match results. If no match results, the firewall sends the query to the default DNS primary and secondary servers. You can enable caching of domains that match the rule.
- **Advanced**—You must enable caching (select **Cache**) and **Cache EDNS Responses** if the DNS proxy object will be used to resolve DNS/FQDN queries that the firewall generates. The Advanced tab also allows you to control TCP queries and UDP Query Retries. The firewall sends TCP or UDP DNS queries through the configured interface. UDP queries switch over to TCP when a DNS query response is too long for a single UDP packet.

DNS Proxy Settings

Click **Add** and configure the firewall to act as a DNS proxy. You can configure a maximum of 256 DNS proxies on a firewall.

DNS Proxy Settings	Configured In	Description
Enable	**DNS Proxy**	Select to enable this DNS proxy.
Name		Specify a name to identify the DNS proxy object (up to **31** characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location		Specify the virtual system to which the DNS proxy object applies: • **Shared**: Proxy applies to all virtual systems. If you choose **Shared**, the **Server Profile** field is not available. Instead, enter the **Primary** and **Secondary** DNS server IP addresses or address objects. • Select a virtual system to use this DNS proxy; you must configure a virtual system first. Select **Device** > **Virtual Systems**, select a virtual system, and select a **DNS Proxy**.
Inheritance Source (Shared location only)		Select a source from which to inherit default DNS server settings. This is commonly used in branch office deployments where the firewall's WAN interface is addressed by DHCP or PPPoE.
Check inheritance source status (Shared location only)		Select to see the server settings that are currently assigned to the DHCP client and PPPoE client interfaces. These may include DNS, WINS, NTP, POP3, SMTP, or DNS suffix.
Primary/Secondary (Shared location only)		Specify the IP addresses of the default primary and secondary DNS servers to which this firewall (as DNS proxy) sends DNS queries. If the primary DNS server cannot be found, the firewall uses the secondary DNS server.
Server Profile (Virtual System location only)		Select or create a new DNS server profile. This field does not appear if the Location of virtual systems was specified as Shared.
Interface		**Add** an interface to function as a DNS proxy. You can add multiple interfaces. To remove the DNS proxy from an interface, select and **Delete** it. An interface is not required if the DNS Proxy is used only for service route functionality. Use a destination service route with a DNS proxy with no interface if you want the destination service route to set the source IP address.

DNS Proxy Settings	Configured In	Description
		Otherwise, the DNS proxy selects an interface IP address to use as a source (when no DNS service routes are set).
Name	**DNS Proxy** > **DNS Proxy Rules**	A name is required so that an entry can be referenced and modified via the CLI.
Turn on caching of domains resolved by this mapping		Select to enable caching of domains that are resolved by this mapping.
Domain Name		**Add** one or more domain names to which the firewall compares incoming FQDNs. If the FQDN matches one of the domains in the rule, the firewall forwards the query to the Primary/Secondary DNS server specified for this proxy. To delete a domain name from the rule, select it and click **Delete**.
DNS Server Profile (Shared location only)		Select or add a DNS server profile to define DNS settings for the virtual system, including the primary and secondary DNS server to which the firewall sends domain name queries.
Primary/Secondary (Virtual System location only)		Enter the hostname or IP address of the primary and secondary DNS servers to which the firewall sends matching domain name queries.
Name	**DNS Proxy** > **Static Entries**	Enter a name for the static entry.
FQDN		Enter the Fully Qualified Domain Name (FQDN) to map to the static IP addresses defined in the Address field.
Address		**Add** one or more IP addresses that map to this domain. The firewall includes all of these addresses in its DNS response, and the client chooses which IP address to use. To delete an address, select the address and click **Delete**.
TCP Queries	**DNS Proxy** > **Advanced**	Select to enable DNS queries using TCP. Specify the maximum number of concurrent pending TCP DNS requests (**Max Pending Requests**) that the firewall will support (range is 64 to 256; default is 64).
UDP Queries Retries	**DNS Proxy** > **Advanced**	Specify settings for UDP query retries: • **Interval**—Time, in seconds, after which the DNS proxy sends another request if it hasn't received a response (range is 1 to 30; default is 2). • **Attempts**—Maximum number of attempts (excluding the first attempt) after which the DNSP tries the next DNS server (range is 1 to 30; default is 5).
Cache	**DNS Proxy** > **Advanced**	You must have **Cache** enabled (enabled by default) if this DNS proxy object is used for queries that the firewall

DNS Proxy Settings	Configured In	Description
		generates (that is, under **Device** > **Setup** > **Services** > **DNS**, or under **Device** > **Virtual Systems** and you select a virtual system and **General** > **DNS Proxy**). Then specify the following: • **Enable TTL**—Limit the length of time the firewall caches DNS entries for the proxy object. TTL is disabled by default. Then enter **Time to Live (sec)**—the number of seconds after which all cached entries for the proxy object are removed and new DNS requests must be resolved and cached again. Range is 60 to 86,400. There is no default TTL; entries remain until the firewall runs out of cache memory. • **Cache EDNS Responses**—You must enable Cache Extension Mechanisms for DNS (EDNS) Responses if this DNS proxy object is used for queries that the firewall generates. The firewall must be able to cache DNS responses in order for the queries for FQDN address objects to succeed.

Additional DNS Proxy Actions

After configuring the firewall as a DNS Proxy, you can perform the following actions on the **Network** > **DNS Proxy** page to manage DNS proxy configurations:

- **Modify**—To modify a DNS proxy, click into the name of the DNS proxy configuration.
- **Delete**—Select a DNS proxy entry and click **Delete** to remove the DNS proxy configuration.
- **Disable**—To disable a DNS proxy, click into the name of the DNS proxy entry and clear the **Enable** option. To enable a DNS proxy that is disabled, click into the name of the DNS proxy entry and select **Enable**.

Network > QoS

The following topics describe Quality of Service (QoS).

What are you looking for?	See:
Set bandwidth limits for an interface and enforce QoS for traffic exiting an interface.	QoS Interface Settings
Monitor traffic exiting a QoS-enabled interface.	QoS Interface Statistics
Looking for more?	See Quality of Service for complete QoS workflows, concepts and use cases.
	Select Policies > QoS to assign matched traffic a QoS class, or select Network > Network Profiles > QoS to define bandwidth limits and priority for up to eight QoS classes.

QoS Interface Settings

Enable QoS on an interface to set bandwidth limits for the interface and/or to enable the interface to enforce QoS for egress traffic. Enabling a QoS interface includes attaching a QoS profile to the interface. QoS is supported on physical interfaces and, depending on firewall model, QoS is also supported on subinterfaces and Aggregate Ethernet (AE) interfaces. See the Palo Alto Networks product comparison tool to view QoS feature support for your firewall model.

To get started, **Add** or modify a QoS Interface, and then configure settings as described in the following table.

QoS Interface Settings	Configured In	Description
Interface Name	**QoS Interface > Physical Interface**	Select the firewall interface on which to enable QoS.
Egress Max (Mbps)		Enter the maximum throughput (in Mbps) for traffic leaving the firewall through this interface. The value is 0 by default, which specifies the firewall limit (60,000 Mbps in PAN-OS 7.1.16 and later releases; 16,000 in PAN-OS 7.1.15 and earlier releases). *Though this is not a required field, we recommend always defining the Egress Max for a QoS interface.*
Turn on QoS feature on this interface		Select to enable QoS on the selected interface.

QoS Interface Settings	Configured In	Description
Clear Text Tunnel Interface Tunnel Interface	**QoS Interface** > **Physical Interface** > **Default Profile**	Select the default QoS profiles for clear text and for tunneled traffic. You must specify a default profile for each. For clear text traffic, the default profile applies to all clear text traffic as an aggregate. For tunneled traffic, the default profile is applied individually to each tunnel that does not have a specific profile assignment in the detailed configuration section. For instructions on defining QoS profiles, refer to Network > Network Profiles > QoS.
Egress Guaranteed (Mbps)	**QoS Interface** > **Clear Text Traffic/ Tunneled Traffic**	Enter the bandwidth that is guaranteed for clear text or tunneled traffic from this interface.
Egress Max (Mbps)		Enter the maximum throughput (in Mbps) for clear text or tunneled traffic leaving the firewall through this interface. The value is 0 by default, which specifies the firewall limit (60,000 Mbps in PAN-OS 7.1.16 and later releases; 16,000 in PAN-OS 7.1.15 and earlier releases). The **Egress Max** for clear text or tunneled traffic must be less than or equal to the **Egress Max** for the physical interface.
Add		• Click **Add** on the **Clear Text Traffic** tab to define additional granularity to the treatment of clear text traffic. Click individual entries to configure the following settings: • **Name**—Enter a name to identify these settings. • **QoS Profile**—Select the QoS profile to apply to the specified interface and subnet. For instructions on defining QoS profiles, refer to Network > Network Profiles > QoS. • **Source Interface**—Select the firewall interface. • **Destination interface**—(PA-3200 Series, PA-5200 Series, PA-7000 Series only) Select the destination interface for which the traffic is intended. • **Source Subnet**—Select a subnet to restrict the settings to traffic coming from that source, or keep the default **any** to apply the settings to any traffic from the specified interface. • Click **Add** from the **Tunneled Traffic** tab to override the default profile assignment for specific tunnels and configure the following settings: • **Tunnel Interface**—Select the tunnel interface on the firewall. • **QoS Profile**—Select the QoS profile to apply to the specified tunnel interface. For example, assume a configuration with two sites, one of which has a 45 Mbps connection and the other a T1 connection to the firewall. You can apply restrictive QoS settings to the T1 site so that the connection is not overloaded while also allowing more flexible settings for the site with the 45 Mbps connection. To remove a clear text or tunneled traffic entry, clear the entry and click **Delete**.

QoS Interface Settings	Configured In	Description
		If the clear text or tunneled traffic sections are left blank, the values specified in the Physical Interface tab's Default Profile section are used.

QoS Interface Statistics

- Network > QoS > Statistics

For a QoS interface, select **Statistics** to view bandwidth, session, and application information for configured QoS interfaces.

QoS Statistics	Description
Bandwidth	Shows the real time bandwidth charts for the selected node and classes. This information is updated every two seconds. *The QoS Egress Max and Egress Guaranteed limitations configured for the QoS classes might be shown with a slightly different value in the QoS statistics screen. This is normal behavior and is due to how the hardware engine summarizes bandwidth limits and counters. There is no operation concern as the bandwidth utilization graphs display the real-time values and quantities.*
Applications	Lists all active applications for the selected QoS node and/or class.
Source Users	Lists all the active source users for the selected QoS node and/or class.
Destination Users	Lists all the active destination users for the selected QoS node and/or class.
Security Rules	Lists the security rules matched to and enforcing the selected QoS node and/or class.
QoS Rules	Lists the QoS rules matched to and enforcing the selected QoS node and/or class.

Network > LLDP

Link Layer Discovery Protocol (LLDP) provides an automatic method of discovering neighboring devices and their capabilities at the Link Layer.

What are you looking for?	See:
What is LLDP?	LLDP Overview
Configure LLDP.	Building Blocks of LLDP
Configure an LLDP profile.	Network > Network Profiles > LLDP Profile
Looking for more?	LLDP

LLDP Overview

LLDP allows the firewall to send and receive Ethernet frames containing LLDP data units (LLDPDUs) to and from neighbors. The receiving device stores the information in a MIB, which can be accessed by the Simple Network Management Protocol (SNMP). LLDP enables network devices to map their network topology and learn capabilities of the connected devices, which makes troubleshooting easier—especially for virtual wire deployments where the firewall would typically go undetected in a network topology.

Building Blocks of LLDP

To enable LLDP on the firewall, click Edit, click **Enable**, and optionally configure the four settings shown in the following table, if the default settings do not suit your environment. The remaining table entries describe the status and peer statistics.

LLDP Settings	Configured In	Description
Transmit Interval (sec)	**LLDP General**	Specify the interval, in seconds, at which LLDPDUs are transmitted (range is 1-3,600; default is 30).
Transmit Delay (sec)		Specify the delay time, in seconds, between LLDP transmissions sent after a change is made in a Type-Length-Value (TLV) element. The delay helps to prevent flooding the segment with LLDPDUs if many network changes spike the number of LLDP changes or if the interface flaps. The **Transmit Delay** must be less than the **Transmit Interval** (range is 1-600; default is 2).
Hold Time Multiple		Specify a value that is multiplied by the **Transmit Interval** to determine the total TTL hold time (range is 1-100; default is 4). The TTL hold time is the length of time the firewall will retain the information from the peer as valid. The maximum TTL hold time is 65,535 seconds, regardless of the multiplier value.

LLDP Settings	Configured In	Description
Notification Interval		Specify the interval, in seconds, at which syslog and SNMP Trap notifications are transmitted when MIB changes occur (range is 1-3,600; default is 5).
spyglass filter	**LLDP** > **Status**	Optionally enter a data value in the filter row and click the gray arrow, which causes only the rows that include that data value to be displayed. Click the red X to Clear Filter.
Interface		Name of the interfaces that have LLDP profiles assigned to them.
LLDP		LLDP status: enabled or disabled.
Mode		LLDP mode of the interface: Tx/Rx, Tx Only, or Rx Only.
Profile		Name of the profile assigned to the interface.
Total Transmitted		Count of LLDPDUs transmitted out the interface.
Dropped Transmit		Count of LLDPDUs that were not transmitted out the interface because of an error. For example, a length error when the system is constructing an LLDPDU for transmission.
Total Received		Count of LLDP frames received on the interface.
Dropped TLV		Count of LLDP frames discarded upon receipt.
Errors		Count of Time-Length-Value (TLV) elements that were received on the interface and contained errors. Types of TLV errors include: one or more mandatory TLVs missing, out of order, containing out-of-range information, or length error.
Unrecognized		Count of TLVs received on the interface that are not recognized by the LLDP local agent, for example, because the TLV type is in the reserved TLV range.
Aged Out		Count of items deleted from the Receive MIB due to proper TTL expiration.
Clear LLDP Statistics		Select to clear all of the LLDP statistics.
spyglass filter	**LLDP** > **Peers**	Optionally enter a data value in the filter row and click the gray arrow, which causes only the rows that include that data value to be displayed. Click the red X to Clear Filter.
Local Interface		Interface on the firewall that detected the neighboring device.
Remote Chassis ID		Chassis ID of the peer; the MAC address is used.

LLDP Settings	Configured In	Description
Port ID	**LLDP** > **Peers (cont)**	Port ID of the peer.
Name		Name of the peer.
More Info		Click **More Info** to see Remote Peer Details, which are based on the Mandatory and Optional TLVs.
Chassis Type		Chassis Type is MAC address.
MAC Address		MAC address of the peer.
System Name		Name of the peer.
System Description		Description of the peer.
Port Description		Port description of the peer.
Port Type		Interface name.
Port ID		Firewall uses the ifname of the interface.
System Capabilities		Capabilities of the system. O=Other, P=Repeater, B=Bridge, W=Wireless-LAN, R=Router, T=Telephone
Enabled Capabilities		Capabilities enabled on the peer.
Management Address		Management address of the peer.

Network > Network Profiles

The following topics describe network profiles:

Network > Network Profiles > GlobalProtect IPSec Crypto

Use the **GlobalProtect IPSec Crypto Profiles** page to specify algorithms for authentication and encryption in VPN tunnels between a GlobalProtect gateway and clients. The order in which you add algorithms is the order in which the firewall applies them, and can affect tunnel security and performance. To change the order, select an algorithm and **Move Up** or **Move Down**.

For VPN tunnels between GlobalProtect gateways and satellites (firewalls), see Network > Network Profiles > IPSec Crypto.

GlobalProtect IPSec Crypto Profile Settings	
Name	Enter a name to identify the profile. The name is case-sensitive, must be unique, and can have up to **31** characters. Use only letters, numbers, spaces, hyphens, and underscores.
Encryption	Click **Add** and select the desired encryption algorithms. For highest security, change the order (top to bottom) to: **aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**.
Authentication	Click **Add** and select the authentication algorithm. Currently, the only option is **sha1**.

Network > Network Profiles > IKE Gateways

Use this page to manage or define a gateway, including the configuration information necessary to perform Internet Key Exchange (IKE) protocol negotiation with a peer gateway. This is the Phase 1 portion of the IKE/IPSec VPN setup.

To manage, configure, restart, or refresh an IKE gateway, see the following:

IKE Gateway Management

- Network > Network Profiles > IKE Gateways

The following table describes how to manage IKE gateways.

Manage IKE Gateways	Description
Add	To create a new IKE gateway, click **Add**. See IKE Gateway General Tab and IKE Gateway Advanced Options Tab for instructions on configuring the new gateway.
Delete	To delete a gateway, select the gateway and click **Delete**.
Enable	To enable a gateway that has been disabled, select the gateway and click **Enable**, which is the default setting for a gateway.
Disable	To disable a gateway, select the gateway and click **Disable**.
PDF/CSV	Administrative roles with a minimum of read-only access can export the object configuration table as **PDF/CSV**. You can apply filters to create more specific table configuration outputs for things such as audits. Only visible columns in the web interface will be exported. See Configuration Table Export.

IKE Gateway General Tab

- Network > Network Profiles > IKE Gateways > General

The following table describes the beginning settings to configure an IKE gateway. IKE is Phase 1 of the IKE/IPSec VPN process. After configuring these settings, see IKE Gateway Advanced Options Tab.

IKE Gateway General Settings	Description
Name	Enter a **Name** to identify the gateway (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Version	Select the IKE version that the gateway supports and must agree to use with the peer gateway: **IKEv1 only mode**, **IKEv2 only mode**, or **IKEv2 preferred mode**. IKEv2 preferred mode causes the gateway to negotiate for IKEv2 and that is what they will use if the peer also supports IKEv2; otherwise, the gateway falls back to IKEv1.
Address Type	Select the type of IP address the gateway uses: **IPv4** or **IPv6**.
Interface	Specify the outgoing firewall interface to the VPN tunnel.
Local IP Address	Select or enter the IP address for the local interface that is the endpoint of the tunnel.

IKE Gateway General Settings	Description
Peer IP Address Type	Select one of the following settings and enter the corresponding information for the peer: • **Dynamic**—Select this option if the peer IP address or FQDN value is unknown. When the peer IP address type is Dynamic, it is up to the peer to initiate the IKE gateway negotiation. • **IP**—Enter **Peer Address** as an IPv4 or IPv6 address or an address object that is an IPv4 or IPv6 address. • **FQDN**—Enter **Peer Address** as an FQDN or an address object that uses an FQDN. If you enter an FQDN or FQDN address object that resolves to more than one IP address, the firewall selects the preferred address from the set of addresses that match the Address Type (IPv4 or IPv6) of the IKE gateway as follows: • If no IKE security association (SA) has been negotiated, the preferred address is the IP address with the smallest value. • If an address is used by the IKE gateway and is in the set of returned addresses, it is used (whether or not it is smallest). • If an address is used by the IKE gateway but isn't in the set of returned addresses, a new address is selected: the smallest address in the set.  *Using an FQDN or FQDN address object reduces issues in environments where the peer is subject to dynamic IP address changes (and would otherwise require you to reconfigure this IKE gateway peer address).*
Authentication	Select the type of authentication: **Pre-Shared Key** or **Certificate** that will occur with the peer gateway. Depending on the selection, see Pre-Shared Key Fields or Certificate Fields.
Pre-Shared Key Fields	
Pre-Shared Key / Confirm Pre-Shared Key	If you select **Pre-Shared Key**, enter a single security key to use for symmetric authentication across the tunnel. The **Pre-Shared Key** value is a string that the administrator creates using a maximum of 255 ASCII or non-ASCII characters. Generate a key that is difficult to crack with dictionary attacks; use a pre-shared key generator, if necessary.
Local Identification	Defines the format and identification of the local gateway, which are used with the pre-shared key for both IKEv1 phase 1 SA and IKEv2 SA establishment. Choose one of the following types and enter the value: **FQDN** (hostname), **IP address**, **KEYID** (binary format ID string in HEX), or **User FQDN** (email address). If you don't specify a value, the gateway will use the local IP address as the **Local Identification** value.

IKE Gateway General Settings	Description
Peer Identification	Defines the type and identification of the peer gateway, which are used with the pre-shared key during IKEv1 phase 1 SA and IKEv2 SA establishment. Choose one of the following types and enter the value: **FQDN** (hostname), **IP address**, **KEYID** (binary format ID string in HEX), or **User FQDN** (email address). If you don't specify a value, the gateway will use the IP address of the peer as the **Peer Identification** value.
Certificate Fields	
Local Certificate	If **Certificate** is selected as the **Authentication** type, from the drop-down, select a certificate that is already on the firewall. Alternatively, you could **Import** a certificate, or **Generate** a new certificate, as follows: **Import**: • **Certificate Name**—Enter a name for the certificate you are importing. • **Shared**—Click if this certificate is to be shared among multiple virtual systems. • **Certificate File**—Click **Browse** to navigate to the location where the certificate file is located. Click on the file and select **Open**. • **File Format**—Select one of the following: • **Base64 Encoded Certificate (PEM)**—Contains the certificate, but not the key. Cleartext. • **Encrypted Private Key and Certificate (PKCS12)**—Contains both the certificate and the key. • **Private key resides on Hardware Security Module**—Click if the firewall is a client of an HSM server where the key resides. • **Import Private Key**—Click if a private key is to be imported because it is in a different file from the certificate file. • **Block Private Key Export**—When you select **Import Private Key**, prevents any administrators, including Superusers, from exporting the private key. • **Key File**—Browse and navigate to the key file to import. This entry is if you chose PEM as the File Format. • **Passphrase** and **Confirm Passphrase**—Enter to access the key.
Local Certificate (cont)	**Generate**: • **Certificate Name**—Enter a name for the certificate you are creating. • **Common Name**—Enter the common name, which is the IP address or FQDN to appear on the certificate. • **Shared**—Click if this certificate is to be shared among multiple virtual systems. • **Signed By**—Select External Authority (CSR) or enter the firewall IP address. This entry must be a CA. • **Certificate Authority**—Click if the firewall is the root CA.

IKE Gateway General Settings	Description
	• **Block Private Key Export**—Prevents any administrators, including Superusers, from exporting the private key. • **OCSP Responder**—Enter the OCSP that tracks whether the certificate is valid or revoked. • **Algorithm**—Select RSA or Elliptic Curve DSA to generate the key for the certificate. • **Number of Bits**—Select 512, 1024, 2048, or 3072 as the number of bits in the key. • **Digest**—Select md5, sha1, sha256, sha384, or sha512 as the method to revert the string from the hash. • **Expiration (days)**—Enter the number of days that the certificate is valid. • **Certificate Attributes**: **Type**—Optionally, select additional attribute types from the drop-down to be in the certificate. • **Value**—Enter a value for the attribute.
HTTP Certificate Exchange	Click **HTTP Certificate Exchange** and enter the **Certificate URL** to use the Hash-and-URL method to tell the peer where to fetch the certificate. The Certificate URL is the URL of the remote server where you store your certificate. If the peer indicates that it also supports Hash and URL, then certificates are exchanged through the SHA1 Hash-and-URL exchange. When the peer receives the IKE certificate payload, it sees the HTTP URL and fetches the certificate from that server. Then the peer uses the hash specified in the certificate payload to check the certificates downloaded from the HTTP server.
Local Identification	Identifies how the local peer is identified in the certificate. Choose one of the following types and enter the value: **Distinguished Name** (Subject), **FQDN** (hostname), **IP address**, or **User FQDN** (email address).
Peer Identification	Identifies how the remote peer is identified in the certificate. Choose one of the following types and enter the value: **Distinguished Name** (Subject), **FQDN** (hostname), **IP address**, or **User FQDN** (email address).
Peer ID Check	Select **Exact** or **Wildcard**. This setting applies to the Peer Identification being examined to validate the certificate. For example, if the Peer Identification is a Name equal to domain.com, you select **Exact**, and the name of the certificate in the IKE ID payload is mail.domain2.com, the IKE negotiation will fail. But if you selected **Wildcard**, then only characters in the Name string before the wildcard asterisk (*) must match and any character after the wildcard can be different.
Permit peer identification and certificate payload identification mismatch	Select if you want the flexibility of having a successful IKE SA even though the peer identification does not match the certificate payload.
Certificate Profile	Select a profile or create a new **Certificate Profile** that configures the certificate options that apply to the certificate that the local gateway sends

IKE Gateway General Settings	Description
	to the peer gateway. See Device > Certificate Management > Certificate Profile.
Enable strict validation of peer's extended key use	Select if you want to strictly control how the key is used.

IKE Gateway Advanced Options Tab

- Network > Network Profiles > IKE Gateways > Advanced Options

Configure advanced IKE gateway settings such as passive mode, NAT Traversal, and IKEv1 settings such as dead peer detection.

IKE Gateway Advanced Options	Description
Enable Passive Mode	Click to have the firewall only respond to IKE connections and never initiate them.
Enable NAT Traversal	Click to have UDP encapsulation used on IKE and UDP protocols, enabling them to pass through intermediate NAT devices. Enable NAT Traversal if Network Address Translation (NAT) is configured on a device between the IPSec VPN terminating points.
IKEv1 Tab	
Exchange Mode	Choose **auto**, **aggressive**, or **main**. In **auto** mode (default), the device can accept both **main** mode and **aggressive** mode negotiation requests; however, whenever possible, it initiates negotiation and allows exchanges in **main** mode. You must configure the peer device with the same exchange mode to allow it to accept negotiation requests initiated from the first device.
IKE Crypto Profile	Select an existing profile, keep the default profile, or create a new profile. The profiles selected for IKEv1 and IKEv2 can differ. For information on IKE Crypto profiles, see Network > Network Profiles > IKE Crypto.
Enable Fragmentation	Click to allow the local gateway to receive fragmented IKE packets. The maximum fragmented packet size is 576 bytes.
Dead Peer Detection	Click to enable and enter an interval (2 - 100 seconds) and delay before retrying (2 - 100 seconds). Dead peer detection identifies inactive or unavailable IKE peers and can help restore resources that are lost when a peer is unavailable.
IKEv2 Tab	

IKE Gateway Advanced Options	Description
IKE Crypto Profile	Select an existing profile, keep the default profile, or create a new profile. The profiles selected for IKEv1 and IKEv2 can differ. For information on IKE Crypto profiles, see Network > Network Profiles > IKE Crypto.
Strict Cookie Validation	Click to enable **Strict Cookie Validation** on the IKE gateway. • When you enable **Strict Cookie Validation**, IKEv2 cookie validation is always enforced; the initiator must send an IKE_SA_INIT containing a cookie. • When you disable **Strict Cookie Validation** (default), the system will check the number of half-open SAs against the global **Cookie Activation Threshold**, which is a VPN Sessions setting. If the number of half-open SAs exceeds the **Cookie Activation Threshold**, the initiator must send an IKE_SA_INIT containing a cookie.
Liveness Check	The IKEv2 **Liveness Check** is always on; all IKEv2 packets serve the purpose of a liveness check. Click this box to have the system send empty informational packets after the peer has been idle for a specified number of seconds. Range: 2-100. Default: 5. If necessary, the side that is trying to send IKEv2 packets attempts the liveness check up to 10 times (all IKEv2 packets count toward the retransmission setting). If it gets no response, the sender closes and deletes the IKE_SA and CHILD_SA. The sender starts over by sending out another IKE_SA_INIT.

IKE Gateway Restart or Refresh

- Network > IPSec Tunnels

Select **Network** > **IPSec Tunnels** to display status of tunnels. In the second Status column is a link to the IKE Info. Click the gateway you want to restart or refresh. The IKE Info page opens. Click one of the entries in the list and click:

- **Restart**—Restarts the selected gateway. A restart will disrupt traffic going across the tunnel. The restart behaviors for IKEv1 and IKEv2 are different, as follows:
  - **IKEv1**—You can restart (clear) a Phase 1 SA or Phase 2 SA independently and only that SA is affected.
  - **IKEv2**—Causes all child SAs (IPSec tunnels) to be cleared when the IKEv2 SA is restarted.

    If you restart the IKEv2 SA, all underlying IPSec tunnels are also cleared.

    If you restart the IPSec Tunnel (child SA) associated with an IKEv2 SA, the restart will not affect the IKEv2 SA.
- **Refresh**—Shows the current IKE SA status.

Network > Network Profiles > IPSec Crypto

Select **Network** > **Network Profiles** > **IPSec Crypto** to configure IPSec Crypto profiles that specify protocols and algorithms for authentication and encryption in VPN tunnels based on IPSec SA negotiation (Phase 2).

For VPN tunnels between GlobalProtect gateways and clients, see Network > Network Profiles > GlobalProtect IPSec Crypto.

IPSec Crypto Profile Settings	Description
Name	Enter a **Name** to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
IPSec Protocol	Select a protocol for securing data that traverses the VPN tunnel: • **ESP**—Encapsulating Security Payload protocol encrypts the data, authenticates the source, and verifies data integrity. • **AH**—Authentication Header protocol authenticates the source and verifies data integrity. *Use ESP protocol because it provides connection confidentiality (encryption) as well as authentication.*
Encryption (ESP protocol only)	Click **Add** and select the desired encryption algorithms. For highest security, use **Move Up** and **Move Down** to change the order (top to bottom) to the following: **aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**, **aes-128-ccm** (the VM-Series firewall doesn't support this option), **aes-128-cbc**, **3des**, and **des**. You can also select **null** (no encryption). *Use a form of AES encryption. (DES and 3DES are weak, vulnerable algorithms.)*
Authentication	Click **Add** and select the desired authentication algorithms. For highest security, use **Move Up** and **Move Down** to change the order (top to bottom) to the following: **sha512**, **sha384**, **sha256**, **sha1**, **md5**. If the **IPSec Protocol** is **ESP**, you can also select **none** (no authentication). *Use sha256 or stronger authentication because md5 and sha1 are not secure. Use sha256 for short-lived sessions and sha384 or higher for traffic that requires the most secure authentication, such as financial transactions.*
DH Group	Select the Diffie-Hellman (DH) group for Internet Key Exchange (IKE): **group1**, **group2**, **group5**, **group14**, **group19**, or **group20**. For highest security, choose the group with the highest number. If you don't want to renew the key that the firewall creates during IKE phase 1, select **no-pfs** (no perfect forward secrecy): the firewall reuses the current key for the IPSec security association (SA) negotiations.
Lifetime	Select units and enter the length of time (default is one hour) that the negotiated key will stay effective.
Lifesize	Select optional units and enter the amount of data that the key can use for encryption.

Network > Network Profiles > IKE Crypto

Use the **IKE Crypto Profiles** page to specify protocols and algorithms for identification, authentication, and encryption (IKEv1 or IKEv2, Phase 1).

To change the order in which an algorithm or group is listed, select the item and then click **Move Up** or **Move Down**. The order determines the first choice when settings are negotiated with a remote peer. The setting at the top of the list is attempted first, continuing down the list until an attempt is successful.

IKE Crypto Profile Settings	Description
Name	Enter a name for the profile.
DH Group	Specify the priority for Diffie-Hellman (DH) groups. Click **Add** and select groups: **group1**, **group2**, **group5**, **group14**, **group19**, or **group20**. For highest security, select an item and then click **Move Up** or **Move Down** to move the groups with higher numeric identifiers to the top of the list. For example, move **group14** above **group2**.
Authentication	Specify the priority for hash algorithms. Click **Add** and select algorithms. For highest security, select an item and then click **Move Up** or **Move Down** to change the order (top to bottom) to the following: • **sha512** • **sha384** • **sha256** • **sha1** • **md5** • (PAN-OS 10.0.3 and later 10.0 releases) **none** *If you select an AES-GCM algorithm for encryption, you must select the Authentication setting none. The hash is automatically selected based on the DH Group selected. DH Group 19 and below uses sha256; DH Group 20 uses sha384.*
Encryption	Select the appropriate Encapsulating Security Payload (ESP) authentication options. Click **Add** and select algorithms. For highest security, select an item and then click **Move Up** or **Move Down** to change the order (top to bottom) to the following: • (PAN-OS 10.0.3 and later 10.0 releases) **aes-256-gcm** (requires IKEv2; DH Group should be set to **group20**) • (PAN-OS 10.0.3 and later 10.0 releases) **aes-128-gcm** (requires IKEv2 and DH Group set to **group19**) • **aes-256-cbc** • **aes-192-cbc** • **aes-128-cbc** • **3des** • **des**

IKE Crypto Profile Settings	Description
	The aes-256-gcm and aes-128-gcm algorithms have authentication built into them; therefore, in those cases you must select the Authentication setting to be none.
Key Lifetime	Select unit of time and enter the length of time that the negotiated IKE Phase 1 key will be effective (default is 8 hours). • IKEv2—Before the key lifetime expires, the SA must be re-keyed or else, upon expiration, the SA must begin a new Phase 1 key negotiation. • IKEv1—Will not actively do a Phase-1 re-key before expiration. Only when the IKEv1 IPSec SA expires will it trigger IKEv1 Phase 1 re-key.
IKEv2 Authentication Multiple	Specify a value (range is 0-50; default is 0) that is multiplied by the Key Lifetime to determine the authentication count. The authentication count is the number of times that the gateway can perform IKEv2 IKE SA re-key before the gateway must start over with IKEv2 re-authentication. A value of 0 disables the re-authentication feature.

Network > Network Profiles > Monitor

A monitor profile is used to monitor IPSec tunnels and to monitor a next-hop device for policy-based forwarding (PBF) rules. In both cases, the monitor profile is used to specify an action to take when a resource (IPSec tunnel or next-hop device) becomes unavailable. Monitor profiles are optional, but can be very useful for maintaining connectivity between sites and to ensure that PBF rules are maintained. The following settings are used to configure a monitor profile.

Field	Description
Name	Enter a name to identify the monitor profile (up to **31** characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Action	Specify an action to take if the tunnel is not available. If the threshold number of heartbeats is lost, the firewall takes the specified action. • **wait-recover**—Wait for the tunnel to recover; do not take additional action. Packets will continue to be sent according to the PBF rule. • **fail-over**—Traffic will fail over to a backup path, if one is available. The firewall uses routing table lookup to determine routing for the duration of this session. In both cases, the firewall tries to negotiate new IPSec keys to accelerate the recovery.
Interval	Specify the time between heartbeats (range is 2 to 10; default is 3).
Threshold	Specify the number of heartbeats to be lost before the firewall takes the specified action (range is 2 to 10; default is 5).

Network > Network Profiles > Interface Mgmt

An Interface Management profile protects the firewall from unauthorized access by defining the services and IP addresses that a firewall interface permits. You can assign an Interface Management profile to Layer 3 Ethernet interfaces (including subinterfaces) and to logical interfaces (aggregate group, VLAN, loopback, and tunnel interfaces). To assign an Interface Management profile, see Network > Interfaces.

Do not attach an interface management profile that allows Telnet, SSH, HTTP, or HTTPS to an interface that allows access from the internet or from other untrusted zones inside your enterprise security boundary. This includes the interface where you have configured a GlobalProtect portal or gateway; GlobalProtect does not require an interface management profile to enable access to the portal or the gateway. Refer to the Best Practices for Securing Administrative Access for details on how to protect access to your firewalls and Panorama.

Do not attach an interface management profile that allows Telnet, SSH, HTTP, or HTTPS to an interface where you have configured a GlobalProtect portal or gateway because this will expose the management interface to the internet.

Field	Description
Name	Enter a profile name (up to **31** characters). This name appears in the list of Interface Management profiles when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Administrative Management Services	• **Telnet**—Use to access the firewall CLI. Telnet uses plaintext, which is not as secure as SSH. *Enable SSH instead of Telnet for management traffic on the interface.* • **SSH**—Use for secure access to the firewall CLI. • **HTTP**—Use to access the firewall web interface. HTTP uses plaintext, which is not as secure as HTTPS. *Enable HTTPS instead of HTTP for management traffic on the interface.* • **HTTPS**—Use for secure access to the firewall web interface.
Network Services	• **Ping**—Use to test connectivity with external services. For example, you can ping the interface to verify it can receive PAN-OS software and content updates from the Palo Alto Networks Update Server. • **HTTP OCSP**—Use to configure the firewall as an Online Certificate Status Protocol (OCSP) responder. For details, see Device > Certificate Management > OCSP Responder. • **SNMP**—Use to process firewall statistics queries from an SNMP manager. For details, see Enable SNMP Monitoring. • **Response Pages**—Use to enable response pages for: • **Authentication Portal**—The ports used to serve Authentication Portal response pages are left open on Layer 3 interfaces: port 6080 for NTLM, 6081 for Authentication Portal without an SSL/TLS Server Profile, and 6082 for Authentication Portal with an SSL/TLS Server Profile. For details, see Device > User Identification > Authentication Portal Settings.

Field	Description
	• **URL Admin Override**—For details, see Device > Setup > Content-ID. • **User-ID**—Use to enable Redistribution of user mappings among firewalls. • **User-ID Syslog Listener-SSL**—Use to allow the PAN-OS integrated User-ID agent to collect syslog messages over SSL. For details, see Configure Access to Monitored Servers. • **User-ID Syslog Listener-UDP**—Use to allow the PAN-OS integrated User-ID agent to collect syslog messages over UDP. For details, see Configure Access to Monitored Servers.
Permitted IP Addresses	Enter the list of IPv4 or IPv6 addresses from which the interface allows access.

Network > Network Profiles > Zone Protection

A Zone Protection profile applied to a zone offers protection against most common floods, reconnaissance attacks, other packet-based attacks, the use of non-IP protocols, and headers with 802.1Q (Ethertype 0x8909) that have specific Security Group Tags (SGTs). A Zone Protection profile is designed to provide broad-based protection at the ingress zone (the zone where traffic enters the firewall) and is not designed to protect a specific end host or traffic going to a particular destination zone. You can attach one zone protection profile to a zone.

Apply a Zone Protection profile to each zone to layer in extra protection against IP floods, reconnaissance, packet-based attacks, and non-IP protocol attacks. Zone Protection on the firewall should be a second layer of protection after a dedicated DDoS device at the internet perimeter.

To augment zone protection capabilities on the firewall, configure a DoS Protection policy (Policies > DoS Protection) to match on a specific zone, interface, IP address, or user.

Zone protection is enforced only when there is no session match for the packet because zone protection is based on new connections per second (cps), not on packets per second (pps). If the packet matches an existing session, it will bypass the zone protection setting.

What are you looking for?	See:
How do I create a Zone Protection profile?	Building Blocks of Zone Protection Profiles Flood Protection Reconnaissance Protection Packet Based Attack Protection Protocol Protection Ethernet SGT Protection

Building Blocks of Zone Protection Profiles

To create a Zone Protection profile, **Add** a profile and name it.

Zone Protection Profile Settings	Configured In	Description
Name	**Network** > **Network Profiles** > **Zone Protection**	Enter a profile name (up to 31 characters). This name appears in the list of Zone Protection profiles when configuring zones. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, and underscores.
Description		Enter an optional description for the Zone Protection profile.

Continue to create the Zone Protection profile by configuring any combination of settings based on what types of protection your zone needs:

- Flood Protection
- Reconnaissance Protection
- Packet Based Attack Protection
- Protocol Protection
- Ethernet SGT Protection

If you have a multi virtual system environment, and have enabled the following:

- *External zones to enable inter virtual system communication*
- *Shared gateways to allow virtual systems to share a common interface and a single IP address for external communications*

the following Zone and DoS protection mechanisms will be disabled on the external zone:

- *SYN cookies*
- *IP fragmentation*
- *ICMPv6*

To enable IP fragmentation and ICMPv6 protection for the shared gateway, you must create a separate Zone Protection profile for the shared gateway.

To protect against SYN floods on a shared gateway, you can apply a SYN Flood protection profile with either Random Early Drop or SYN cookies; on an external zone, only Random Early Drop is available for SYN Flood protection.

Flood Protection

- Network > Network Profiles > Zone Protection > Flood Protection

Configure a profile that provides flood protection against SYN, ICMP, ICMPv6, SCTP INIT, and UDP packets, as well as protection against flooding from other types of IP packets. The rates are in connections per second; for example, an incoming SYN packet that doesn't match an existing session is considered a new connection.

Zone Protection Profile Settings—Flood Protection	Configured In	Description
SYN	**Network** > **Network Profiles** > **Zone**	Select to enable protection against SYN floods.

Zone Protection Profile Settings—Flood Protection	Configured In	Description
Action	**Protection** > **Flood Protection**	Select the action to take in response to a SYN flood attack. • **Random Early Drop**—Causes SYN packets to be dropped to mitigate a flood attack: • When the flow exceeds the **Alert** rate threshold, an alarm is generated. • When the flow exceeds the **Activate** rate threshold, the firewall drops individual SYN packets randomly to restrict the flow. • When the flow exceeds the **Maximum** rate threshold, 100% of incoming SYN packets are dropped. • **SYN Cookies**—Causes the firewall to act like a proxy, intercept the SYN, generate a cookie on behalf of the server to which the SYN was directed, and send a SYN-ACK with the cookie to the original source. Only when the source returns an ACK with the cookie to the firewall does the firewall consider the source valid and forward the SYN to the server. This is the preferred Action.  *SYN Cookies treats legitimate traffic fairly but consumes more firewall resources than RED. If SYN Cookies consumes too many resources, switch to RED. If you don't have a dedicated DDoS prevention device in front of the firewall (at the internet perimeter), always use RED.*
Alarm Rate (connections/sec)	**Network** > **Network Profiles** > **Zone Protection** > **Flood Protection** (cont)	Enter the number of SYN packets (not matching an existing session) the zone receives per second that triggers an alarm. You can view alarms on the Dashboard and in the threat log (Monitor > Packet Capture). Range is 0-2,000,000; default is 10,000. The best practice is to set the threshold to 15-20% above the average zone CPS rate to accommodate normal fluctuations and adjust the threshold if you receive too many alarms.
Activate (connections/sec)		Enter the number of SYN packets (not matching an existing session) that the zone receives per second that triggers the Action specified in this Zone Protection profile. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the Maximum rate. The firewall stops dropping the SYN

Zone Protection Profile Settings—Flood Protection	Configured In	Description
		packets if the incoming rate drops below the Activate threshold. Range is 1 to 2,000,000; default is 10,000. The best practice is to set the threshold just above the zone's peak CPS rate to avoid throttling legitimate traffic and adjust the threshold as needed.
Maximum (connections/sec)		Enter the maximum number of SYN packets (not matching an existing session) that the zone receives per second before packets exceeding the maximum are dropped. Range is 1 to 2,000,000; default is 40,000. Crossing this threshold blocks new connections until the CPS rate falls below the threshold. The best practice is to set the threshold to 80-90% of firewall capacity, taking into account other features that consume firewall resources.
ICMP	**Network** > **Network Profiles** > **Zone Protection** > **Flood Protection** (cont)	Select to enable protection against ICMP floods.
Alarm Rate (connections/sec)		Enter the number of ICMP echo requests (pings not matching an existing session) that the zone receives per second that triggers an attack alarm. Range is 0-2,000,000; default is 10,000. The best practice is to set the threshold to 15-20% above the average zone CPS rate to accommodate normal fluctuations and adjust the threshold if you receive too many alarms.
Activate (connections/sec)		Enter the number of ICMP packets (not matching an existing session) that the zone receives per second before subsequent ICMP packets are dropped. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the Maximum rate. The firewall stops dropping the ICMP packets if the incoming rate drops below the Activate threshold. Range is 1 to 2,000,000; default is 10,000. The best practice is to set the threshold just above the zone's peak CPS rate to avoid throttling legitimate traffic and adjust the threshold as needed.
Maximum (connections/sec)		Enter the maximum number of ICMP packets (not matching an existing session) that the zone receives per second before packets exceeding the maximum are dropped. Range is 1 to 2,000,000; default is 40,000. The best practice is to set the threshold to 80-90% of firewall capacity, taking into account other features that consume firewall resources.

Zone Protection Profile Settings—Flood Protection	Configured In	Description
SCTP INIT	**Network** > **Network Profiles** > **Zone Protection** > **Flood Protection** (cont)	Select to enable protection against floods of Stream Control Transmission Protocol (SCTP) packets that contain an Initiation (INIT) chunk. An INIT chunk cannot be bundled with other chunks, so the packet is referred to as an SCTP INIT packet.
Alarm Rate (connections/sec)		Enter the number of SCTP INIT packets (not matching an existing session) that the zone receives per second that triggers an attack alarm. Range is 0-2,000,000. Default per firewall model is: • **PA-5280**—10,000 • **PA-5260**—7,000 • **PA-5250**—5,000 • **PA-5220**—3,000 • **VM-700**—1,000 • **VM-500**—500 • **VM-300**—250 • **VM-100**—200 • **VM-50**—100
Activate (connections/sec)		Enter the number of SCTP INIT packets (not matching an existing session) that the zone receives per second before subsequent SCTP INIT packets are dropped. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the Maximum rate. The firewall stops dropping SCTP INIT packets if the incoming rate drops below the Activate threshold. Range is 1 to 2,000,000. Default per firewall model is the same as for Alarm Rate.
Maximum (connections/sec)	**Network** > **Network Profiles** > **Zone Protection** > **Flood Protection** (cont)	Enter the maximum number of SCTP INIT packets (not matching an existing session) that the zone receives per second before packets exceeding the maximum are dropped. Range is 1 to 2,000,000. Default per firewall model is: • **PA-5280**—20,000 • **PA-5260**—14,000 • **PA-5250**—10,000 • **PA-5220**—6,000 • **VM-700**—2,000 • **VM-500**—1,000 • **VM-300**—500 • **VM-100**—400 • **VM-50**—200

Zone Protection Profile Settings—Flood Protection	Configured In	Description
UDP	**Network** > **Network Profiles** > **Zone Protection** > **Flood Protection** (cont)	Select to enable protection against UDP floods.
Alarm Rate (connections/sec)		Enter the number of UDP packets (not matching an existing session) that the zone receives per second that triggers an attack alarm. Range is 0-2,000,000; default is 10,000. The best practice is to set the threshold to 15-20% above the average zone CPS rate to accommodate normal fluctuations and adjust the threshold if you receive too many alarms.
Activate (connections/sec)		Enter the number of UDP packets (not matching an existing session) that the zone receives per second that triggers random dropping of UDP packets. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the Maximum rate. The firewall stops dropping the UDP packets if the incoming rate drops below the Activate threshold. Range is 1 to 2,000,000; default is 10,000. The best practice is to set the threshold just above the zone's peak CPS rate to avoid throttling legitimate traffic and adjust the threshold as needed.
Maximum (connections/sec)		Enter the maximum number of UDP packets (not matching an existing session) the zone receives per second before packets exceeding the maximum are dropped. Range is 1 to 2,000,000; default is 40,000. The best practice is to set the threshold to 80-90% of firewall capacity, taking into account other features that consume firewall resources.
ICMPv6	**Network** > **Network Profiles** > **Zone Protection** > **Flood Protection** (cont)	Select to enable protection against ICMPv6 floods.
Alarm Rate (connections/sec)		Enter the number of ICMPv6 echo requests (pings not matching an existing session) that the zone receives per second that triggers an attack alarm. Range is 0-2,000,000; default is 10,000. The best practice is to set the threshold to 15-20% above the average zone CPS rate to accommodate normal fluctuations and adjust the threshold if you receive too many alarms.
Activate (connections/sec)		Enter the number of ICMPv6 packets (not matching an existing session) that the zone receives per second before subsequent ICMPv6 packets are dropped. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the Maximum

Zone Protection Profile Settings—Flood Protection	Configured In	Description
		rate. The firewall stops dropping the ICMPv6 packets if the incoming rate drops below the Activate threshold. Range is 1 to 2,000,000; default is 10,000. The best practice is to set the threshold just above the zone's peak CPS rate to avoid throttling legitimate traffic and adjust the threshold as needed.
Maximum (connections/sec)		Enter the maximum number of ICMPv6 packets (not matching an existing session) that the zone receives per second before packets exceeding the maximum are dropped. Range is 1 to 2,000,000; default is 40,000. The best practice is to set the threshold to 80-90% of firewall capacity, taking into account other features that consume firewall resources.
Other IP	**Network** > **Network Profiles** > **Zone Protection** > **Flood Protection** (cont)	Select to enable protection against other IP (non-TCP, non-ICMP, non-ICMPv6, non-SCTP, and non-UDP) floods.
Alarm Rate (connections/sec)		Enter the number of other IP packets (non-TCP, non-ICMP, non-ICMPv6, non-SCTP, and non-UDP packets) (not matching an existing session) the zone receives per second that triggers an attack alarm. Range is 0-2,000,000; default is 10,000. The best practice is to set the threshold to 15-20% above the average zone CPS rate to accommodate normal fluctuations and adjust the threshold if you receive too many alarms.
Activate (connections/sec)		Enter the number of other IP packets (non-TCP, non-ICMP, non-ICMPv6, and non-UDP packets) (not matching an existing session) the zone receives per second that triggers random dropping of other IP packets. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the Maximum rate. The firewall stops dropping the Other IP packets if the incoming rate drops below the Activate threshold. Range is 1 to 2,000,000; default is 10,000. The best practice is to set the threshold just above the zone's peak CPS rate to avoid throttling legitimate traffic and adjust the threshold as needed.
Maximum (connections/sec)		Enter the maximum number of other IP packets (non-TCP, non-ICMP, non-ICMPv6, and non-UDP packets) (not matching an existing session) the zone receives per second before packets exceeding the maximum are dropped. Range is 1 to 2,000,000; default is 40,000.

Zone Protection Profile Settings—Flood Protection	Configured In	Description
		The best practice is to set the threshold to 80-90% of firewall capacity, taking into account other features that consume firewall resources.

Reconnaissance Protection

- Network > Network Profiles > Zone Protection > Reconnaissance Protection

The following settings define reconnaissance protection:

Zone Protection Profile Settings—Reconnaissance Protection	Configured In	Description
TCP Port Scan	**Network** > **Network Profiles** > **Zone Protection** > **Reconnaissance Protection**	**Enable** configures the profile to enable protection against TCP port scans.
UDP Port Scan		**Enable** configures the profile to enable protection against UDP port scans.
Host Sweep		**Enable** configures the profile to enable protection against host sweeps.
Action		Action that the system will take in response to the corresponding reconnaissance attempt: • **Allow**—Permits the port scan or host sweep reconnaissance. • **Alert**—Generates an alert for each port scan or host sweep that matches the threshold within the specified time interval (the default action). • **Block**—Drops all subsequent packets from the source to the destination for the remainder of the specified time interval. • **Block IP**—Drops all subsequent packets for the specified **Duration**, in seconds (range is 1-3,600). **Track By** determines whether to block source or source-and-destination traffic. For example, block attempts above the threshold number per interval that are from a single source (more stringent), or block attempts that have a source and destination pair (less stringent). *Block all Reconnaissance scans except your internal vulnerability testing scans.*
Interval (sec)		Time interval, in seconds, for TCP or UDP port scan detection (range is 2-65,535; default is 2).

Zone Protection Profile Settings—Reconnaissance Protection	Configured In	Description
		Time interval, in seconds, for host sweep detection (range is 2-65,535; default is 10).
Threshold (events)		Number of scanned port events or host sweep events within the specified time interval that triggers the Action (range is 2-65,535; default is 100).  *Use the default event threshold to log a few packets for analysis before blocking reconnaissance attempts.*
Source Address Exclusion		IP addresses that you want to exclude from reconnaissance protection. The list supports a maximum of 20 IP addresses or Netmask address objects. • **Name**—Enter a descriptive name for the address to exclude. • **Address Type**—Select IPv4 or IPv6 from the drop-down. • **Address**—Select an address or address object from the drop-down or enter one manually.  *Exclude only IP addresses for trusted internal groups that perform vulnerability testing.*

Packet Based Attack Protection

- Network > Network Profiles > Zone Protection > Packet Based Attack Protection

You can configure Packet Based Attack protection to drop the following types of packets:

- IP Drop
- TCP Drop
- ICMP Drop
- IPv6 Drop
- ICMPv6 Drop

IP Drop

To instruct the firewall what to do with certain IP packets it receives in the zone, specify the following settings.

Zone Protection Profile Settings—Packet Based Attack Protection	Configured In	Description
Spoofed IP address	**Network** > **Network Profiles** > **Zone Protection** > **Packet Based Attack Protection** > **IP Drop**	Check that the source IP address of the ingress packet is routable and the routing interface is in the same zone as the ingress interface. If either condition is not true, discard the packet.  *On internal zones only, drop spoofed IP address packets to ensure that on ingress, the source address matches the firewall routing table.*
Strict IP Address Check		Check that both conditions are true: • The source IP address is not the subnet broadcast IP address of the ingress interface. • The source IP address is routable over the exact ingress interface. If either condition is not true, discard the packet. For a firewall in Common Criteria (CC) mode, you can enable logging for discarded packets. On the firewall web interface, select **Device** > **Log Settings**. In the Manage Logs section, select **Selective Audit** and enable **Packet Drop Logging**.
Fragmented traffic		Discard fragmented IP packets.
IP Option Drop		Select the settings in this group to enable the firewall to drop packets containing these IP Options.
Strict Source Routing		Discard packets with the Strict Source Routing IP option set. Strict Source Routing is an option whereby a source of a datagram provides routing information through which a gateway or host must send the datagram.  *Drop packets with strict source routing because source routing allows adversaries to bypass Security policy rules that use the destination IP address as the matching criteria.*
Loose Source Routing		Discard packets with the Loose Source Routing IP option set. Loose Source Routing is an option whereby a source of a datagram provides routing information and a gateway or host is allowed to choose any route of a number of intermediate gateways to get the datagram to the next address in the route.  *Drop packets with loose source routing because source routing allows adversaries to bypass*

Zone Protection Profile Settings—Packet Based Attack Protection	Configured In	Description
		Security policy rules that use the destination IP address as the matching criteria.
Timestamp		Discard packets with the Timestamp IP option set.
Record Route		Discard packets with the Record Route IP option set. When a datagram has this option, each router that routes the datagram adds its own IP address to the header, thus providing the path to the recipient.
Security		Discard packets if the security option is defined.
Stream ID		Discard packets if the Stream ID option is defined.
Unknown		Discard packets if the class and number are unknown.  *Discard unknown packets.*
Malformed		Discard packets if they have incorrect combinations of class, number, and length based on RFCs 791, 1108, 1393, and 2113.  *Discard malformed packets.*

TCP Drop

To instruct the firewall what to do with certain TCP packets it receives in the zone, specify the following settings.

Zone Protection Profile Settings—Packet Based Attack Protection	Configured In	Description
Mismatched overlapping TCP segment	**Network** > **Network Profiles** > **Zone Protection** > **Packet Based Attack Protection** > **TCP Drop**	Attackers can construct connections with overlapping but different data in them to cause misinterpretation of the connection. Attackers can use IP spoofing and sequence number prediction to intercept a user's connection and inject their own data. Use this setting to report an overlap mismatch and drop the packet when segment data does not match in these scenarios: • The segment is within another segment. • The segment overlaps with part of another segment.

Zone Protection Profile Settings—Packet Based Attack Protection	Configured In	Description
		• The segment covers another segment. This protection mechanism uses sequence numbers to determine where packets reside within the TCP data stream.  *Drop packets with mismatched overlapping TCP segments.*
Split Handshake		Prevent a TCP session from being established if the session establishment procedure does not use the well-known three-way handshake. A four-way or five-way split handshake or a simultaneous open session establishment procedure are examples of variations that would not be allowed. The Palo Alto Networks next-generation firewall correctly handles sessions and all Layer 7 processes for split handshake and simultaneous open session establishment without configuring **Split Handshake**. When this is configured for a zone protection profile and the profile is applied to a zone, TCP sessions for interfaces in that zone must be established using the standard three-way handshake; the variations are not allowed.  *Drop packets with split handshakes.*
TCP SYN with Data		Prevent a TCP session from being established if the TCP SYN packet contains data during a three-way handshake. Enabled by default.
TCP SYNACK with Data		Prevent a TCP session from being established if the TCP SYN-ACK packet contains data during a three-way handshake. Enabled by default.
Reject Non-SYN TCP		Determine whether to reject the packet if the first packet for the TCP session setup is not a SYN packet: • **global**—Use system-wide setting that is assigned through **TCP Settings** or the CLI. • **yes**—Reject non-SYN TCP. • **no**—Accept non-SYN TCP.  *Allowing non-SYN TCP traffic may prevent file blocking policies from working as expected in cases where the client and/or server connection is not set after the block occurs.*  *If you configure Tunnel Content Inspection on a zone and enable Rematch Sessions, then for that*

Zone Protection Profile Settings—Packet Based Attack Protection	Configured In	Description
		zone only, disable Reject Non-SYN TCP so that enabling or editing a Tunnel Content Inspection policy doesn't cause the firewall to drop existing tunnel sessions.
Asymmetric Path		Determine whether to drop or bypass packets that contain out-of-sync ACKs or out-of-window sequence numbers: • **global**—Use system-wide setting that is assigned through **TCP Settings** or the CLI. • **drop**—Drop packets that contain an asymmetric path. • **bypass**—Bypass scanning on packets that contain an asymmetric path.
Strip TCP Options		Determine whether to strip the TCP Timestamp or TCP Fast Open option from TCP packets.
TCP Timestamp	**Network** > **Network Profiles** > **Zone Protection** > **Packet Based Attack Protection** > **TCP Drop**	Determine whether the packet has a TCP timestamp in the header and, if it does, strip the timestamp from the header. *Strip the TCP timestamp from packets that have it to prevent a timestamp DoS attack.*
TCP Fast Open		Strip the TCP Fast Open option (and data payload, if any) from the TCP SYN or SYN-ACK packet during a TCP three-way handshake. When this is cleared (disabled), the TCP Fast Open option is allowed, which preserves the speed of a connection setup by including data delivery. This functions independently of the TCP SYN with Data and TCP SYN-ACK with Data. Disabled by default.
Multipath TCP (MPTCP) Options		MPTCP is an extension of TCP that allows a client to maintain a connection by simultaneously using multiple paths to connect to the destination host. By default, MPTCP support is disabled, based on the global MPTCP setting. Review or adjust the MPTCP settings for the security zones associated with this profile: • **no**—Enable MPTCP support (do not strip the MPTCP option). • **yes**—Disable MPTCP support (strip the MPTCP option). With this configured, MPTCP connections are converted to standard TCP connections, as MPTCP is backwards compatible with TCP. • **(Default) global**—Support MPTCP based on the global MPTCP setting. By default, the global MPTCP setting is set to yes so that MPTCP is disabled (the MPTCP option is stripped from the packet). You can review or adjust the global MPTCP setting

Zone Protection Profile Settings—Packet Based Attack Protection	Configured In	Description
		using the **Strip MPTCP option** in **TCP Settings** or through the following CLI command: `# set deviceconfig setting tcp strip-mptcp-option <yes|no>`

ICMP Drop

To instruct the firewall to drop certain ICMP packets it receives in the zone, select the following settings to enable them.

Zone Protection Profile Settings—Packet Based Attack Protection	Configured In	Description
ICMP Ping ID 0	**Network** > **Network Profiles** > **Zone Protection** > **Packet Based Attack Protection** > **ICMP Drop**	Discard packets if the ICMP ping packet has an identifier value of 0.
ICMP Fragment		Discard packets that consist of ICMP fragments.
ICMP Large Packet (>1024)		Discard ICMP packets that are larger than 1024 bytes.
Discard ICMP embedded with error message		Discard ICMP packets that are embedded with an error message.
Suppress ICMP TTL Expired Error		Stop sending ICMP TTL expired messages.
Suppress ICMP Frag Needed		Stop sending ICMP fragmentation needed messages in response to packets that exceed the interface MTU and have the do not fragment (DF) bit set. This setting will interfere with the PMTUD process performed by hosts behind the firewall.

IPv6 Drop

To instruct the firewall to drop certain IPv6 packets it receives in the zone, select the following settings to enable them.

Zone Protection Profile Settings—Packet Based Attack Protection	Configured In	Description
Type 0 Routing Heading	**Network** > **Network Profiles** > **Zone Protection** > **Packet Based Attack Protection** > **IPv6 Drop**	Discard IPv6 packets containing a Type 0 routing header. See RFC 5095 for Type 0 routing header information.
IPv4 compatible address		Discard IPv6 packets that are defined as an RFC 4291 IPv4-Compatible IPv6 address.
Anycast source address		Discard IPv6 packets that contain an anycast source address.
Needless fragment header		Discard IPv6 packets with the last fragment flag (M=0) and offset of zero.
MTU in ICMP 'Packet Too Big' less than 1280 bytes		Discard IPv6 packets that contain a Packet Too Big ICMPv6 message when the maximum transmission unit (MTU) is less than 1,280 bytes.
Hop-by-Hop extension		Discard IPv6 packets that contain the Hop-by-Hop Options extension header.
Routing extension		Discard IPv6 packets that contain the Routing extension header, which directs packets to one or more intermediate nodes on its way to its destination.
Destination extension		Discard IPv6 packets that contain the Destination Options extension, which contains options intended only for the destination of the packet.
Invalid IPv6 options in extension header		Discard IPv6 packets that contain invalid IPv6 options in an extension header.
Non-zero reserved field		Discard IPv6 packets that have a header with a reserved field not set to zero.

ICMPv6 Drop

To instruct the firewall what to do with certain ICMPv6 packets it receives in the zone, select the following settings to enable them.

Zone Protection Profile Settings—Packet Based Attack Protection	Configured In	Description
ICMPv6 destination unreachable - require explicit security rule match	**Network** > **Network Profiles** > **Zone Protection** > **Packet Based Attack Protection** > **ICMPv6 Drop**	Require an explicit Security policy match for Destination Unreachable ICMPv6 messages, even when the message is associated with an existing session.
ICMPv6 packet too big - require explicit security rule match		Require an explicit Security policy match for Packet Too Big ICMPv6 messages, even when the message is associated with an existing session.
ICMPv6 time exceeded - require explicit security rule match		Require an explicit Security policy match for Time Exceeded ICMPv6 messages, even when the message is associated with an existing session.
ICMPv6 parameter problem - require explicit security rule match		Require an explicit Security policy match for Parameter Problem ICMPv6 messages, even when the message is associated with an existing session.
ICMPv6 redirect - require explicit security rule match		Require an explicit Security policy match for Redirect Message ICMPv6 messages, even when the message is associated with an existing session.

Protocol Protection

- Network > Network Profiles > Zone Protection > Protocol Protection

The firewall normally allows non-IP protocols between Layer 2 zones and between virtual wire zones. Protocol protection allows you to control which non-IP protocols are allowed (include) or denied (exclude) between or within security zones on a Layer 2 VLAN or virtual wire. Examples of non-IP protocols include AppleTalk, Banyan VINES, Novell, NetBEUI, and Supervisory Control and Data Acquisition (SCADA) systems such as Generic Object Oriented Substation Event (GOOSE).

After you configure protocol protection in a Zone Protection profile, apply the profile to an ingress security zone on a Layer 2 VLAN or virtual wire.

Enable Protocol Protection on internet-facing zones to prevent layer 2 traffic from protocols you don't use from getting on your network.

Zone Protection Profile Settings—Protocol Protection	Configured In	Description
Rule Type	**Network** > **Network Profiles** > **Zone Protection** > **Protocol Protection**	Specify the type of list you are creating for protocol protection: • **Include List**—Only the protocols on the list are allowed—in addition to IPv4 (0x0800), IPv6 (0x86DD), ARP (0x0806), and VLAN tagged frames (0x8100). All other protocols are implicitly denied (blocked). • **Exclude List**—Only the protocols on the list are denied; all other protocols are implicitly allowed. You cannot exclude IPv4 (0x0800), IPv6 (0x86DD), ARP (0x0806), or VLAN tagged frames (0x8100).  *Use the Include List to allow only the layer 2 protocols you use and to deny all other protocols. This reduces the attack surface by denying the protocols you don't use on the network. The firewall denies only the protocols that you add to the Exclude List and allows all other protocols that are not on the list. If you don't configure Protocol Protection, all layer 2 protocols are allowed.*
Protocol Name		Enter the protocol name that corresponds to the Ethertype code you are adding to the list. The firewall does not verify that the protocol name matches the Ethertype code but the Ethertype code does determine the protocol filter.
Enable		**Enable** the Ethertype code on the list. If you want to disable a protocol for testing purposes but not delete it, disable it, instead.
Ethertype (hex)		Enter an Ethertype code (protocol) preceded by 0x to indicate hexadecimal (range is 0x0000 to 0xFFFF). A list can have a maximum of 64 Ethertypes. Some sources of Ethertype codes are: • IEEE hexadecimal Ethertype • standards.ieee.org/develop/regauth/ethertype/eth.txt • http://www.cavebear.com/archive/cavebear/Ethernet/type.html

Ethernet SGT Protection

- Network > Network Profiles > Zone Protection > Ethernet SGT Protection

For a firewall in a Cisco TrustSec network, create a Zone Protection profile with a list of Layer 2 Security Group Tags (SGTs) that you want to exclude. Apply the Zone Protection profile to a Layer 2, virtual wire, or tap interface. If an incoming packet with an 802.1Q (Ethertype 0x8909) header has an SGT that matches an SGT in your list, the firewall drops the packet.

Zone Protection Profile Settings	Configured In	Description
Layer 2 SGT Exclude List	**Network** > **Network Profiles** > **Zone Protection** > **Ethernet SGT Protection**	Enter a name for the list of Security Group Tags (SGTs).
Tag		Enter the Layer 2 SGTs in headers of packets that you want to exclude (drop) when the SGT matches this list in the Zone Protection profile applied to a zone (range is 0 to 65,535).
Enable		**Enable** (default) this exclude list for Ethernet SGT protection. De-select the **Enable** option to disable the exclude list.

Network > Network Profiles > QoS

Add a QoS profile to define the bandwidth limits and priority for up to eight classes of service. You can set both guaranteed and maximum bandwidth limits for individual classes and for the collective classes. Priorities determine how traffic is treated in the presence of contention.

To fully enable the firewall to provide QoS, also:

- Define the traffic that you want to receive QoS treatment (select Policies > QoS to add or modify a QoS policy).
- Enable QoS on an interface (select Network > QoS).

See Quality of Service for complete QoS workflows, concepts, and use cases.

QoS Profile Settings	
Profile Name	Enter a name to identify the profile (up to **31** characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Egress Max	Enter the maximum throughput (in Mbps) for traffic leaving the firewall through this interface. The value is 0 by default, which specifies the firewall limit (60,000 Mbps in PAN-OS 7.1.16 and later releases; 16,000 in PAN-OS 7.1.15 and earlier releases). The **Egress Max** for a QoS profile must be less than or equal to the **Egress Max** for the physical interface enabled with QoS. See Network > QoS. *Though this is not a required field, it is recommended to always define the Egress Max for a QoS profile.*
Egress Guaranteed	Enter the bandwidth that is guaranteed for this profile (Mbps). When the egress guaranteed bandwidth is exceeded, the firewall passes traffic on a best-effort basis.

QoS Profile Settings	
Classes	**Add** and specify how to treat individual QoS classes. You can select one or more classes to configure: • **Class**—If you do not configure a class, you can still include it in a QoS policy. In this case, the traffic is subject to overall QoS limits. Traffic that does not match a QoS policy will be assigned to class 4. • **Priority**—Click and select a priority to assign it to a class: • **real-time** • **high** • **medium** • **low** When contention occurs, traffic that is assigned a lower priority is dropped. Real-time priority uses its own separate queue. • **Egress Max**—Click and enter the maximum throughput (in Mbps) for this class. The value is 0 by default, which specifies the firewall limit (60,000 Mbps in PAN-OS 7.1.16 and later releases; 16,000 in PAN-OS 7.1.15 and earlier releases). The **Egress Max** for a QoS class must be less than or equal to the **Egress Max** for the QoS profile.  *Though this is not a required field, we recommend you always define the Egress Max value for a QoS profile.* • **Egress Guaranteed**—Click and enter the guaranteed bandwidth (Mbps) for this class. Guaranteed bandwidth assigned to a class is not reserved for that class—bandwidth that is unused continues to remain available to all traffic. However, when the egress guaranteed bandwidth for a traffic class is exceeded, the firewall passes that traffic on a best-effort basis.

Network > Network Profiles > LLDP Profile

A Link Layer Discovery Protocol (LLDP) profile is the way in which you configure the LLDP mode of the firewall, enable syslog and SNMP notifications, and configure the optional Type-Length-Values (TLVs) you want transmitted to LLDP peers. After configuring the LLDP profile, you assign the profile to one or more interfaces.

Learn more about LLDP, including how to configure and monitor LLDP.

LLDP Profile Settings	Description
Name	Specify a name for the LLDP profile.
Mode	Select the mode in which LLDP will function: **transmit-receive**, **transmit-only**, or **receive-only**.
SNMP Syslog Notification	Enables SNMP trap and syslog notifications, which will occur at the global **Notification Interval**. If enabled, the firewall will send both an SNMP trap and a syslog event as configured in the **Device** > **Log Settings** > **System** > **SNMP Trap Profile** and **Syslog Profile**.

LLDP Profile Settings	Description
Port Description	Enables the ifAlias object of the firewall to be sent in the Port Description TLV.
System Name	Enables the sysName object of the firewall to be sent in the System Name TLV.
System Description	Enables the sysDescr object of the firewall to be sent in the System Description TLV.
System Capabilities	Enables the deployment mode (L3, L2, or virtual wire) of the interface to be sent, via the following mapping, in the System Capabilities TLV. • If L3, the firewall advertises router (bit 6) capability and the Other bit (bit 1). • If L2, the firewall advertises MAC Bridge (bit 3) capability and the Other bit (bit 1). • If virtual wire, the firewall advertises Repeater (bit 2) capability and the Other bit (bit 1). SNMP MIB will combine capabilities configured on interfaces into a single entry.
Management Address	Enables the **Management Address** to be sent in the Management Address TLV. You can enter up to four management addresses, which are sent in the order they are specified. To change the order, click **Move Up** or **Move Down**.
Name	Specify a name for the Management Address.
Interface	Select an interface whose IP address will be the Management Address. If you select **None**, you can enter an IP address in the field next to the IPv4 or IPv6 selection.
IP Choice	Select **IPv4** or **IPv6**, and in the adjacent field, select or enter the IP address to be transmitted as the Management Address. At least one management address is required if **Management Address** TLV is enabled. If no management IP address is configured, the system uses the MAC address of the transmitting interface as the management address transmitted.

Network > Network Profiles > BFD Profile

Bidirectional Forwarding Detection (BFD) enables extremely fast detection of a link failure, which accelerates failover to a different route.

What are you looking for?	See:
What is BFD?	BFD Overview
What fields are available to create a BFD profile?	Building Blocks of a BFD Profile
View BFD status for a virtual router.	View BFD Summary and Details
Looking for more?	Learn more about and configure BFD.

What are you looking for?	See:
	Configure BFD for: Static Routes BGP OSPF OSPFv3 RIP

BFD Overview

BFD is a protocol that recognizes a failure in the bidirectional path between two forwarding engines, such as interfaces, data links, or the actual forwarding engines. In the PAN-OS implementation, one of the forwarding engines is an interface on the firewall and the other is an adjacent configured BFD peer. The BFD failure detection between two engines is extremely fast, providing faster failover than could be achieved by link monitoring or frequent dynamic routing health checks, such as Hello packets or heartbeats.

After BFD detects a failure, it notifies the routing protocol to switch to an alternate path to the peer. If BFD is configured for a static route, the firewall removes the affected routes from the RIB and FIB tables.

BFD is supported on the following interface types: physical Ethernet, AE, VLAN, tunnel (Site-to-Site VPN and LSVPN), and subinterfaces of Layer 3 interfaces. For each static route or dynamic routing protocol, you can enable or disable BFD, select the default BFD profile, or configure a BFD profile.

Building Blocks of a BFD Profile

- Network > Network Profiles > BFD Profile

You can enable BFD for a static route or dynamic routing protocol by applying the default BFD profile or a BFD profile that you create. The default profile uses the default BFD settings and cannot be changed. You can **Add** a new BFD profile and specify the following information.

BFD Profile Settings	Description
Name	Name of the BFD profile (up to 31 characters). The name is case-sensitive and must be unique on the firewall. Use only letters, numbers, spaces, hyphens, and underscores.
Mode	Mode in which BFD operates: • **Active**—BFD initiates sending control packets (default). At least one of the BFD peers must be active; they can both be active. • **Passive**—BFD waits for the peer to send control packets and responds as required.
Desired Minimum Tx Interval (ms)	Minimum interval (in milliseconds) at which you want the BFD protocol to send BFD control packets. Minimum value on PA-7000 Series is 50; minimum on PA#3200 Series is 100; minimum on VM-Series is 200 (maximum value is 2000; default is 1000).

BFD Profile Settings	Description
	If you have multiple protocols that use different BFD profiles on the same interface, configure the BFD profiles with the same Desired Minimum Tx Interval.
Required Minimum Rx Interval (ms)	Minimum interval (in milliseconds) at which BFD can receive BFD control packets. Minimum value on PA-7000 Series is 50; minimum on PA-3200 Series is 100; minimum on VM-Series is 200 (maximum value is 2000; default is 1000).
Detection Time Multiplier	The local system calculates the detection time as the **Detection Time Multiplier** received from the remote system multiplied by the agreed transmit interval of the remote system (the greater of the **Required Minimum Rx Interval** and the last received **Desired Minimum Tx Interval**). If BFD does not receive a BFD control packet from its peer before the detection time expires, a failure has occurred (range is 2 to 50; default is 3).
Hold Time (ms)	Delay (in milliseconds) after a link comes up before the firewall transmits BFD control packets. **Hold Time** applies to BFD Active mode only. If the firewall receives BFD control packets during the **Hold Time**, it ignores them (range is 0-120000; default is 0). The default setting of 0 means no transmit **Hold Time** is used; the firewall sends and receives BFD control packets immediately after the link is established.
Enable Multihop	Enables BFD over multiple hops. Applies to BGP implementation only.
Minimum Rx TTL	Minimum Time-to-Live value (number of hops) BFD will accept (receive) when it supports multihop BFD. Applies to BGP implementation only (range is 1-254; there is no default).

View BFD Summary and Details

- Network > Virtual Routers

The following table describes BFD summary information.

View BFD Information	
View a BFD summary.	Select **Network** > **Virtual Routers** and in the row of the virtual router you are interested in, click **More Runtime Stats**. Select the **BFD Summary Information** tab.
View BFD details.	Select **details** in the row of the interface you are interested in to view BFD Details.

Network > Network Profiles > SD-WAN Interface Profile

Create an SD-WAN Interface Profile to group physical links by Link Tag and to control the speed of links and how frequently the firewall monitors the link.

	SD-WAN Interface Profile
Name	Enter the name of the SD-WAN Interface Profile using a maximum of 31 alphanumeric characters. The name must begin with an alphanumeric character and can contain letters, numbers, underscores (_), hyphens (-), periods (.), and spaces.
Link Tag	Select the Link Tag that this profile will assign to the interface or add a new tag. A link tag bundles physical links (different ISPs) for the firewall to select from during path selection and failover.
Description	It is a best practice to enter a user-friendly description of the profile.
Link Type	Select the physical link type from the predefined list (**ADSL/DSL**, **Cable Modem**, **Ethernet**, **Fiber**, **LTE/3G/4G/5G**, **MPLS**, **Microwave/Radio**, **Satellite**, **WiFi**, or **Other**). The firewall can support any CPE device that terminates and hands off as an Ethernet connection to the firewall; for example, WiFi access points, LTE modems, laser-microwave CPEs all can terminate with an Ethernet hand-off.
Maximum Download (Mbps)	Enter the maximum download speed from the ISP in megabits per second; range is 1 to 100,000, there is no default value. Ask your ISP for the link speed or sample the link's maximum speeds with a tool such as speedtest.net and take an average of the maximums over a good length of time.
Maximum Upload (Mbps)	Enter the maximum upload speed from the ISP in megabits per second; range is 1 to 100,000, there is no default value. Ask your ISP for the link speed or sample the link's maximum speeds with a tool such as speedtest.net and take an average of the maximums over a good length of time.
Eligible for Error Correction Profile interface selection	Select this setting to make interfaces (where you apply this profile) eligible for the encoding firewall to select them for Forward Error Correction (FEC) or packet duplication. You can deselect this setting so that expensive FEC or packet duplication is never used on an expensive link (interface) where you apply the profile. The **Link Type** specified for the profile determines whether the default setting of **Eligible for Error Correction Profile interface selection** is selected or not. To configure FEC or packet duplication, create an SD-WAN Error Correction Profile.
VPN Data Tunnel Support	Determines whether the branch-to-hub traffic and the return traffic flows through a VPN tunnel for added security (enabled by default) or flows outside of the VPN tunnel to avoid encryption overhead. • Leave **VPN Data Tunnel Support** enabled for public link types that have direct internet connections or internet breakout capability, such as cable modem, ADSL, and other internet connections. • You can disable **VPN Data Tunnel Support** for private link types such as MPLS, satellite, or microwave that do not have internet breakout capability. However, you must first ensure the traffic cannot be intercepted because it will be sent outside of the VPN tunnel. • The branch many have DIA traffic that needs to fail over to the private MPLS link connecting to the hub, and reach the internet from the hub. The **VPN Data Tunnel Support** setting determines whether the private data flows through the VPN tunnel or flows outside the tunnel, and the failed over traffic uses

	SD-WAN Interface Profile
	the other connection (that the private data flow doesn't use). The firewall uses zones to segment DIA failover traffic from private MPLS traffic.
VPN Failover Metric	(PAN-OS 10.0.3 and later 10.0 releases) When you configure DIA AnyPath, you need a way to specify the failover order of individual VPN tunnels bundled in a hub virtual interface or branch virtual interface to which DIA fails over. Specify the VPN Failover Metric for the VPN tunnel (link); range is 1 to 65,535; default is 10. The lower the metric value, the higher the priority of the tunnel (link where you apply this profile) to be chosen during failover. For example, set the metric to a low value and apply the profile to a broadband interface; then create a different profile that sets a high metric to apply to an expensive LTE interface to ensure it is used only after broadband has failed over.
Path Monitoring	Select the path monitoring mode in which the firewall monitors the interfaces where you apply this SD-WAN Interface Profile. • **Aggressive**—(default for all link types except LTE and Satellite) Firewall sends probe packets to the opposite end of the SD-WAN link at a constant frequency. *Use Aggressive mode if you need fast detection and failover for brownout and blackout conditions.* • **Relaxed**—(default for LTE and Satellite link types) Firewall waits for a number of seconds (the **Probe Idle Time**) between sending sets of probe packets, making path monitoring less frequent. When the Probe Idle Time expires, the firewall sends probes for seven seconds at the **Probe Frequency** configured. *Use Relaxed mode when you have low bandwidth links, links that charge by usage (such as LTE), or when fast detection isn't as important as preserving cost and bandwidth.*
Probe Frequency (per second)	Enter the probe frequency, which is the number of times per second that the firewall sends a probe packet to the opposite end of the SD-WAN link (range is 1 to 5; default is 5).
Probe Idle Time (seconds)	If you select **Relaxed** path monitoring, you can set the probe idle time (in seconds) that the firewall waits between sets of probe packets (range is 1 to 60; default is 60).
Failback Hold Time (seconds)	Enter the length of time (in seconds) that the firewall waits for a recovered link to remain qualified before the firewall reinstates that link as the preferred link after it has failed over (range is 20 to 120; default is 120). The failback hold time prevents a recovered link from being reinstated as the preferred link too quickly and having it fail again right away.

Device

Use the following sections for field reference on basic system configuration and maintenance tasks on the firewall:

- Device > Setup
- Device > High Availability
- Device > Log Forwarding Card
- Device > Config Audit
- Device > Password Profiles
- Device > Administrators
- Device > Admin Roles
- Device > Access Domain
- Device > Authentication Profile
- Device > Authentication Sequence
- Device > User Identification
- Device > Data Redistribution
- Device > Device Quarantine
- Device > VM Information Sources
- Device > Troubleshooting
- Device > Virtual Systems
- Device > Shared Gateways
- Device > Certificate Management
- Device > Response Pages
- Device > Log Settings
- Device > Server Profiles
- Device > Local User Database > Users
- Device > Local User Database > User Groups
- Device > Scheduled Log Export
- Device > Software
- Device > GlobalProtect Client
- Device > Dynamic Updates
- Device > Licenses
- Device > Support
- Device > Master Key and Diagnostics
- Device > Policy Recommendation

Device > Setup

Device > Setup > Management

- **Device** > **Setup** > **Management**
- **Panorama** > **Setup** > **Management**

On a firewall, select **Device** > **Setup** > **Management** to configure management settings.

On Panorama™, select **Device** > **Setup** > **Management** to configure firewalls that you manage with Panorama templates. Select **Panorama** > **Setup** > **Management** to configure management settings for Panorama.

The following management settings apply to both the firewall and Panorama except where noted.

- General Settings
- Authentication Settings
- Policy Rulebase Settings
- Panorama Settings: Device > Setup > Management (settings configured on the firewall to connect to Panorama)
- Panorama Settings: Panorama > Setup > Management (settings configured on Panorama for connections to firewalls)
- Logging and Reporting Settings
- Banners and Messages
- Minimum Password Complexity
- AutoFocus™
- Cortex Data Lake
- SSH Management Profiles Settings

Item	Description
General Settings	
Hostname	Enter a hostname (up to 31 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores. If you don't enter a value, PAN-OS® uses the firewall model (for example, PA-5220_2) as the default. Optionally, you can configure the firewall to use a hostname that a DHCP server provides. See Accept DHCP server-provided Hostname (Firewall only). *Configure a unique host name to easily identify the device you are managing.*
Domain	Enter the name of the network domain for the firewall (up to 31 characters). Optionally, you can configure the firewalls and Panorama to use a domain that a DHCP server provides. See Accept DHCP server-provided Domain (Firewall only).

Item	Description
Accept DHCP server-provided Hostname (Firewall only)	(Applies only when the Management Interface IP Type is DHCP Client) Select this option to have the management interface accept the hostname it receives from the DHCP server. The hostname from the server (if valid) overwrites any value specified in the Hostname field.
Accept DHCP server-provided Domain (Firewall only)	(Applies only when the Management Interface IP Type is DHCP Client) Select this option to have the management interface accept the domain (DNS suffix) it receives from the DHCP server. The domain from the server overwrites any value specified in the **Domain** field.
Login Banner	Enter text (up to 3,200 characters) to display on the web interface login page below the **Name** and **Password** fields.
Force Admins to Acknowledge Login Banner	Select this option to display and force administrators to select **I Accept and Acknowledge the Statement Below** (above the login banner on the login page), which forces administrators to acknowledge that they understand and accept the contents of the message before they can **Login**.
SSL/TLS Service Profile	Assign an existing SSL/TLS Service profile or create a new one to specify a certificate and the SSL/TLS protocol settings allowed on the management interface (see Device > Certificate Management > SSL/TLS Service Profile). The firewall or Panorama uses this certificate to authenticate to administrators who access the web interface through the management (MGT) interface or through any other interface that supports HTTP/HTTPS management traffic (see Network > Network Profiles > Interface Mgmt). If you select **none** (default), the firewall or Panorama uses a predefined certificate. *The predefined certificate is provided for convenience. For better security, assign an SSL/TLS Service profile. To ensure trust, the certificate must be signed by a certificate authority (CA) certificate that is in the trusted root certificate store of the client systems.*
Time Zone	Select the time zone of the firewall.
Locale	Select a language for PDF reports from the drop-down. See Monitor > PDF Reports > Manage PDF Summary. Even if you have a specific language preference set for the web interface, PDF reports will use the language specified for **Locale**.
Date	Set the date on the firewall; enter the current date (in YYYY/MM/DD format) or select the date from the drop-down.

Item	Description
	You can also define an NTP server (Device > Setup > Services).
Time	Set the time on the firewall; enter the current time) in 24-hour format) or select the time from the drop-down. *You can also define an NTP server (Device > Setup > Services).*
Serial Number (Panorama virtual appliances only)	Enter the serial number for Panorama. You can find the serial number in the order fulfillment email you received from Palo Alto Networks®.
Latitude	Enter the latitude (-90.0 to 90.0) of the firewall.
Longitude	Enter the longitude (-180.0 to 180.0) of the firewall.
Automatically acquire commit lock	Select this option to automatically apply a commit lock when you change the candidate configuration. For more information, see Lock Configurations. *Enable Automatically Acquire Commit Lock so that other administrators can't make configuration changes until the first administrator commits her/his changes.*
Certificate Expiration Check	Instruct the firewall to create warning messages when on-box certificates approach their expiration date. *Enable Certificate Expiration Check to generate a warning message when on-box certificates approach their expiration date.*
Multiple Virtual System Capability	Enables the use of multiple virtual systems on firewalls that support this feature (see Device > Virtual Systems). *To enable multiple virtual systems on a firewall, firewall policies must reference no more than 640 distinct user groups. If necessary, reduce the number of referenced user groups. Then, after you enable and add multiple virtual systems, the policies can then reference another 640 user groups for each additional virtual system.*
URL Filtering Database (Panorama only)	Select a URL Filtering vendor for use with Panorama: **brightcloud** or **paloaltonetworks** (PAN-DB).

Item	Description
Use Hypervisor Assigned MAC Addresses (VM-Series firewalls only)	Select this option to have the VM-Series firewall use the MAC address that the hypervisor assigned, instead of generating a MAC address using the PAN-OS custom schema. If you enable this option and use an IPv6 address for the interface, the interface ID cannot use the EUI-64 format, which derives the IPv6 address from the interface MAC address. In a high availability (HA) active/passive configuration, a commit error occurs if you use the EUI-64 format.
GTP Security	Select this option to enable the ability to inspect the control plane and user dataplane messages in the GPRS Tunneling Protocol (GTP) traffic. See Objects > Security Profiles > Mobile Network Protection to configure a Mobile Network Protection profile so that you can enforce policy on GTP traffic.
SCTP Security	Select this option to enable the ability to inspect and filter Stream Control Transmission Protocol (SCTP) packets and chunks, and to apply SCTP initiation (INIT) flood protection. See Objects > Security Profiles > SCTP Protection. For SCTP INIT flood protection, see Configure SCTP INIT Flood Protection.
Advanced Routing	Select this option to enable the advanced routing engine, which supports BGP and static routes. You must commit and reboot the firewall for the change to the new routing engine to take effect (or to change back to the legacy route engine).  *Advanced Routing is in preview mode and that feature set is limited.*
Tunnel Acceleration	Select this option to improve performance and throughput for traffic going through GRE tunnels, VXLAN tunnels, and GTP-U tunnels This option is enabled by default. • **GRE and VXLAN tunnel acceleration**—Supported on PA-3200 Series firewalls and PA-7000 Series firewalls with PA-7000-NPC and SMC-B. • **GTP-U tunnel acceleration**—Supported on PA-7000 Series firewalls with PA-7000-NPC and SMC-B. For GTP-U tunnel traffic to have tunnel acceleration, Tunnel Acceleration must be enabled, GTP must be enabled, no tunnel content inspection (TCI) policy rules for GTP-U protocol can be configured, and a Security policy rule with a Mobile Network Protection profile attached must allow the GTP traffic.  *If you disable or re-enable Tunnel Acceleration and commit, you must reboot the firewall.*
Device Certificate	
Get certificate	Click to enter the One Time Password (OTP) generated from the Palo Alto Networks Customer Support Portal. The device

Item	Description
	certificate is required to successfully authenticate Panorama with the CSP and leverage cloud services such as Zero Touch Provisioning (ZTP), IoT, Device Telemetry, and Enterprise Data Loss Prevention (DLP). After you successfully install the device certificate, the following is displayed: • **Current Device Certificate Status**—The current status of device certificate (`Valid`, `Invalid`, or `Expired`) • **Not Valid Before**—Timestamp indicating when the device certificate validity begins. • **Not Valid After**—Timestamp indicating when the device certificate validity expires and the device certificate becomes `Invalid` or `Expired`. • **Last Fetched Message**—Message displaying the whether the device certificate is successfully installed or if the device certificate installation failed. • **Last Fetched Status**—The status of fetching the device certificate (`success` or `failed`). • **Last Fetched Timestamp**—Timestamp of the last device certificate installation attempt.
Authentication Settings	
Authentication Profile	Select the authentication profile (or sequence) the firewall uses to authenticate administrative accounts that you define on an external server instead of locally on the firewall (see Device > Authentication Profile). When external administrators log in, the firewall requests authentication and authorization information (such as the administrative role) from the external server. Enabling authentication for external administrators requires additional steps based on the server type that the authentication profile specifies, which must be one of the following: • RADIUS • TACACS+ • SAML *Administrators can use SAML to authenticate to the web interface but not to the CLI.* Select **None** to disable authentication for external administrators. For administrative accounts that you define locally (on the firewall), the firewall authenticates using the authentication profile assigned to those accounts (see Device > Administrators).
Certificate Profile	Select a certificate profile to verify the client certificates of administrators who are configured for certificate-based access to the firewall web interface. For instructions on configuring certificate profiles, see Device > Certificate Management > Certificate Profile.

Item	Description
	Configure a certificate profile to ensure that the administrator's host machine has the right certificates to authenticate with the Root CA certificate defined in the certificate profile.
Idle Timeout	Enter the maximum time (in minutes) without any activity on the web interface or CLI before an administrator is automatically logged out (range is 0 to 1,440; default is 60). A value of 0 means that inactivity does not trigger an automatic logout. *Both manual and automatic refreshing of web interface pages (such as the Dashboard and System Alarms dialog) reset the Idle Timeout counter. To enable the firewall to enforce the timeout when you are on a page that supports automatic refreshing, set the refresh interval to Manual or to a value higher than the Idle Timeout. You can also disable Auto Refresh in the ACC tab.* *Set the Idle Timeout to 10 minutes to prevent unauthorized users from accessing the firewall if an administrator leaves a firewall session open.*
API Key Lifetime	Enter the length of time (in minutes) for which the API key is valid (range is 0 to 525,600; default is 0). A value of 0 means that the API key never expires. **Expire All API Keys** to invalidate all previously generated API keys. Use this option with caution because all existing keys are rendered useless and any operation where you are currently using those API keys will stop functioning. *Perform this operation during a maintenance window so that you can replace the keys without disrupting current implementations where you referenced the API keys.*
API Keys Last Expired	Displays the timestamp of when the API key last expired. This field has no value if you have never reset your keys.
Failed Attempts	Enter the number of failed login attempts (0 to 10) that the firewall allows for the web interface and CLI before locking out the administrator account. A value of 0 specifies unlimited login attempts. The default value is 0 for firewalls in normal operational mode and 10 for firewalls in FIPS-CC mode. Limiting login attempts can help protect the firewall from brute force attacks. *If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, the Failed*

Item	Description
	Attempts is ignored and the user is never locked out. *Set the number of Failed Attempts to 5 or fewer to accommodate a reasonable number of retries in case of typing errors, while preventing malicious systems from trying brute force methods to log in to the firewall.*
Lockout Time	Enter the number of minutes (range is 0 to 60) for which the firewall locks out an administrator from access to the web interface and CLI after reaching the **Failed Attempts** limit. A value of 0 (default) means the lockout applies until another administrator manually unlocks the account. *If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, the user is locked out after the set number of failed login attempts until another administrator manually unlocks the account.* *Set the Lockout Time to at least 30 minutes to prevent continuous login attempts from a malicious actor.*
Max Session Count	Enter the number of concurrent sessions allowed for all administrator and user accounts (range is 0 to 4). A value of 0 (default) means that an unlimited amount of concurrent sessions are allowed. *In FIPS-CC mode, the range is 1 to 4 with a default value of 4.*
Max Session Time	Enter the number of minutes (range is 60 to 1,499) that an active, non-idle administrator can remain logged in. Once this max session time is reached, the session is terminated and requires re-authentication to begin another session. The default value is set to 0 (30 days), which cannot be manually entered. If no value is entered, the **Max Session Time** defaults to 0. *In FIPS-CC mode, the range is 60 to 1,499 and the default value is 720. If no value is entered, the Max Session Time defaults to 720.*
Policy Rulebase Settings	
Require Tag on Policies	Requires at least one tag when creating a new policy rule. If a policy rule already exists when you enable this option, you must add at least one tag the next time you edit the rule.

Item	Description
Require Description on Policies	Requires that you add a **Description** when you create a new policy rule. If a policy rule already exists when you enable this option, you must add a **Description** the next time you edit the rule.
Fail Commit if Policies Have No Tags or Descriptions	Forces your commit to fail if you do not add any tags or a description to the policy rule. If a policy rule already exists when you enable this option, the commit will fail if no tag or description are added the next time you edit the rule. To fail the commit, you must **Require tag on policies** or **Require description on policies**.
Require Audit Comment on Policies	Requires **Audit Comment** when creating a new policy rule. If a policy rule already exists when you enable this option, you must add **Audit Comment** the next time you edit the rule.
Audit Comment Regular Expression	Specify requirements for the comment format parameters in audit comments.
Policy Rule Hit Count	Tracks how often traffic matches the policy rules you configured on the firewall. When enabled, you can view the total Hit Count for total traffic matches against each rule along with the date and time when the rule was Created, Modified, was First Hit and Last Hit.
Policy Application Usage	

Panorama Settings: Device > Setup > Management

Configure the following settings on the firewall or in a template on Panorama. These settings establish a connection from the firewall to Panorama.

You must also configure connection and object sharing settings on Panorama (Panorama Settings: Panorama > Setup > Management).

The firewall uses an SSL connection with AES256 encryption to register with Panorama. By default, Panorama and the firewall authenticate each other using predefined 2,048-bit certificates and they use the SSL connection for configuration management and log collection. To further secure the SSL connections between Panorama, firewalls, and log collectors, see Secure Client Communication *to configure custom certificates between the firewall and Panorama or a log collector.*

Panorama Servers	Enter the IP address or FQDN of the Panorama server. If Panorama is in a high availability (HA) configuration, in the second **Panorama Servers** field, enter the IP address or FQDN of the secondary Panorama server.
Receive Timeout for Connection to Panorama	Enter the timeout (in seconds) for receiving TCP messages from Panorama (range is 1 to 240; default is 240).

Item	Description
Send Timeout for Connection to Panorama	Enter the timeout (in seconds) for sending TCP messages to Panorama (range is 1 to 240; default is 240).
Retry Count for SSL Send to Panorama	Enter the number of retry attempts allowed when sending Secure Socket Layer (SSL) messages to Panorama (range is 1 to 64; default is 25).
Enable Automated Commit Recovery	Enable to enable the firewall to automatically verify its connection to the Panorama management server when a configuration is committed and pushed to the firewall, and at configured intervals after a configuration is successfully pushed. When enabled, and the firewall fails to verify its connection to the Panorama management server, the firewall and Panorama management automatically revert their configuration to the previous running configuration to restore connectivity.
Number of attempts to check for Panorama connectivity	When **Enabled Automated Commit Recovery** is enabled, configure the number of times the firewall tests its connection to the Panorama management server.
Interval between retries (sec)	When **Enable Automated Commit Recovery** is enabled, configure the time in seconds between the number of attempts the firewall tests its connection to the Panorama management server.
Secure Client Communication	Enable **Secure Client Communication** to ensure that the firewall uses configured custom certificates (instead of the default certificate) to authenticate SSL connections with Panorama or log collectors. • **None** (default)—No device certificate is configured and the default predefined certificate is used. • **Local**—The firewall uses a local device certificate and the corresponding private key generated on the firewall or imported from an existing enterprise PKI server. • **Certificate**—Select the local device certificate you generated or imported. This certificate can be unique to the firewall (based on a hash of the serial number of that firewall) or it can be a common device certificate used by all firewalls that connect to Panorama. • **Certificate Profile**—Select the Certificate Profile from the drop-down. The Certificate Profile defines the CA certificate for verifying client certificates and how to verify certificate revocation status. • **SCEP**—The firewall uses a device certificate and private key generated by a Simple Certificate Enrollment Protocol (SCEP) server. • **SCEP Profile**—Select a Device > Certificate Management > SCEP from the drop-down. The SCEP Profile provides Panorama with the necessary information to authenticate client devices against a SCEP server in your enterprise PKI.

Item	Description
	• **Certificate Profile**—Select the Device > Certificate Management > Certificate Profile from the drop-down. The Certificate Profile defines the CA certificate for verifying client certificates and how to verify certificate revocation status.
	• **Customize Communication**—The firewall uses its configured custom certificate to authenticate with the selected devices. • **Panorama Communication**—The firewall uses the configured client certificate for communication with Panorama. • **PAN-DB Communication**—The firewall uses the configured client certificate for communication with a PAN-DB appliance. • **WildFire Communication**—The firewall uses the configured client certificate for communication with a WildFire® appliance. • **Log Collector Communication**—The firewall uses the configured client certificate for communication with a Log Collector. • **Check Server Identity**—(Panorama and Log Collector Communication only) The firewall confirms the identify of the server by matching the common name (CN) with the IP address or FQDN of the server.
Disable/Enable Panorama Policy and Objects	This option displays only when you edit the **Panorama Settings** on a firewall (not in a template on Panorama). **Disable Panorama Policy and Objects** to disable the propagation of device group policies and objects to the firewall. By default, this action also removes those policies and objects from the firewall. To keep a local copy of the device group policies and objects on the firewall, in the dialog that opens when you click this option, select **Import Panorama Policy and Objects before disabling**. After you perform a commit, these policies and objects become part of the firewall configuration and Panorama no longer manages them. Under normal operating conditions, disabling Panorama management is unnecessary and could complicate the maintenance and configuration of firewalls. This option generally applies to situations where firewalls require rules and object values that differ from those defined in the device group. An example is when you move a firewall out of production and into a laboratory environment for testing. To revert firewall policy and object management to Panorama, click **Enable Panorama Policy and Objects**.
Disable/Enable Device and Network Template	This option displays only when you edit the **Panorama Settings** on a firewall (not in a template on Panorama). **Disable Device and Network Template** to disable the propagation of template information (device and network configurations) to

Item	Description
	the firewall. By default, this action also removes the template information from the firewall. To keep a local copy of the template information on the firewall, in the dialog that opens when you select this option, select **Import Device and Network Templates before disabling**. After you perform a commit, the template information becomes part of the firewall configuration and Panorama no longer manages that information. *Under normal operating conditions, disabling Panorama management is unnecessary and could complicate the maintenance and configuration of firewalls. This option generally applies to situations where firewalls require device and network configuration values that differ from those defined in the template. An example is when you move a firewall out of production and into a laboratory environment for testing.* To configure the firewall to accept templates again, click **Enable Device and Network Templates**.

Panorama Settings: Panorama > Setup > Management

If you use Panorama to manage firewalls, configure the following settings on Panorama. These settings determine timeouts and SSL message attempts for the connections from Panorama to managed firewalls, as well as object sharing parameters.

You must also configure Panorama connection settings on the firewall or in a template on Panorama: see Panorama Settings: Device > Setup > Management.

The firewall uses an SSL connection with AES256 encryption to register with Panorama. By default, Panorama and the firewall authenticate each other using predefined 2,048-bit certificates and they use the SSL connection for configuration management and log collection. To further secure these SSL connections, see Customize Secure Server Communication to configure custom certificates between Panorama and its clients.

Receive Timeout for Connection to Device	Enter the timeout (in seconds) for receiving TCP messages from all managed firewalls (range is 1 to 240; default is 240).
Send Timeout for Connection to Device	Enter the timeout (in seconds) for sending TCP messages to all managed firewalls (range is 1 to 240; default is 240).
Retry Count for SSL Send to Device	Enter the number of allowed retry attempts when sending Secure Socket Layer (SSL) messages to managed firewalls (range is 1 to 64; default is 25).
Share Unused Address and Service Objects with Devices	Select this option (enabled by default) to share all Panorama shared objects and device-group-specific objects with managed firewalls. If you disable this option, the appliance checks Panorama policies for references to address, address group, service, and service group objects, and does not share any unreferenced objects.

Item	Description
	This option reduces the total object count by ensuring that the appliance sends only necessary objects to managed firewalls. If you have a policy rule that targets specific devices in a device group, then the objects used in that policy are considered used in that device group.
Objects defined in ancestors will take higher precedence	Select this option (disabled by default) to specify that the object values in ancestor groups take precedence over those in descendant groups when device groups at different levels in the hierarchy have objects of the same type and name but with different values. This means that when you perform a device group commit, the ancestor values replace any override values. Likewise, this option causes the value of a shared object to override the values of objects of the same type and name in device groups. Selecting this option displays the Find Overridden Objects link.
Find Overridden Objects	Select this option (bottom of the Panorama Settings dialog) to list any *shadowed* objects. A shadowed object is an object in the Shared location that has the same name but a different value in a device group. The link displays only if you specify that Objects defined in ancestors will take higher precedence.
Enable reporting and filtering on groups	Select this option (disabled by default) to enable Panorama to locally store usernames, user group names, and username-to-group mapping information that it receives from firewalls. This option is global to all device groups in Panorama. However, you must also enable local storage at the level of each device group by specifying a Master Device and configuring the firewall to Store users and groups from Master Device.
Secure Communication Settings: Panorama > Setup > Management	
Customize Secure Server Communication	• **Custom Certificate Only**—When enabled, Panorama accepts only custom certificates for authentication with managed firewalls and Log Collectors. • **SSL/TLS Service Profile**—Select an SSL/TLS service profile from the drop-down. This profile defines the certificate and supported SSL/TLS versions that the firewall can use to communicate with Panorama. • **Certificate Profile**—Select a certificate profile from the drop-down. This certificate profile defines certificate revocation-checking behavior and the root CA used to authenticate the certificate chain presented by the client. • **Authorization List**—**Add** and configure a new authorization profile using the following fields to set the criteria for authorizing client devices that can connect to Panorama. The Authorization List supports a maximum of 16 profile entries. • **Identifier**—Select **Subject** or **Subject Alt. Name** as the authorization identifier.

Item	Description
	• **Type**—If you selected **Subject Alt. Name** as the Identifier, then select **IP**, **hostname**, or **e-mail** as the identifier type. If you selected **Subject**, then you must use **common name** as the identifier type. • **Value**—Enter the identifier value. • **Authorize Clients Based on Serial Number**—Panorama authorizes client devices based on a hash of the device serial number. • **Check Authorization List**—Panorama checks client device identities against the authorization list. A device need match only one criterion on the list to be authorized. If no match is found, the device is not authorized. • **Disconnect Wait Time (min)**—The amount of time (in minutes) that Panorama waits before terminating the current connection with its managed devices. Panorama then reestablishes connections with its managed devices using the configured secure server communications settings. The wait time begins after you commit the secure server communications configuration.
Secure Client Communications	Using **Secure Client Communication** ensures that the client Panorama uses configured custom certificates (instead of the default predefined certificate) to authenticate SSL connections with another Panorama appliance in an HA pair or WildFire appliance. • **Predefined** (default)—No device certificate is configured and Panorama uses the default predefined certificate. • **Local**—Panorama uses a local device certificate and the corresponding private key generated on the firewall or imported from an existing enterprise PKI server. • **Certificate**—Select the local device certificate. • **Certificate Profile**—Select the Certificate Profile from the drop-down. • **SCEP**—Panorama uses a device certificate and private key generated by a Simple Certificate Enrollment Protocol (SCEP) server. • **SCEP Profile**—Select a SCEP Profile from the drop-down. • **Certificate Profile**—Select the Certificate Profile from the drop-down. • **Customize Communication** • **HA Communication**—Panorama uses the configured client certificate for HA communication with its HA peer. • **WildFire Communication**—Panorama uses the configured client certificate for communication with a WildFire appliance.
Logging and Reporting Settings Use this section to modify:	

Item	Description
• Expiration periods and storage quotas for reports and for the following log types. The settings are synchronized across high availability pairs. • Logs of all types that the firewall generates and stores locally (**Device** > **Setup** > **Management**). The settings apply to all the virtual systems on the firewall. • Logs that an M-Series appliance or a Panorama virtual appliance in Panorama mode generates and stores locally: System, Config, Application Statistics, and User-ID™ logs (**Panorama** > **Setup** > **Management**). • Logs of all types that the Panorama virtual appliance in Legacy mode generates locally or collects from firewalls (**Panorama** > **Setup** > **Management**). *For the logs that firewalls send to Panorama Log Collectors, you set storage quotas and expiration periods in each Collector Group (see Panorama > Collector Groups).* • Attributes for calculating and exporting user activity reports. • Predefined reports created on the firewall or Panorama.	
Log Storage tab (Panorama management server and all firewall models except PA-5200 Series and PA#7000 Series firewalls) *Panorama displays this tab if you edit the Logging and Reporting Settings (Panorama > Setup > Management). If you use a Panorama template to configure the settings for firewalls (Device > Setup > Management), see Single Disk Storage and Multi Disk Storage tabs.*	For each log type, specify: • **Quota**—The **Quota**, as a percentage, allocated on the hard disk for log storage. When you change a **Quota** value, the associated disk allocation changes automatically. If the total of all the values exceeds 100%, a message appears in red and an error message will appear if you try to save the settings. If this happens, adjust the percentages so that the total is within the 100% limit. *VM-Series firewalls by default have a 0% quota allocated for SCTP log storage, SCTP Summary, Hourly SCTP Summary, Daily SCTP Summary, and Weekly SCTP Summary, so you must allocate some percentage for these firewalls to log SCTP information.* • **Max Days**—The length (in days) of the log expiration period (range is 1 to 2,000). The firewall or Panorama appliance automatically deletes logs that exceed the specified period. By default, there is no expiration period, which means logs never expire. The firewall or Panorama appliance evaluates logs during creation of the logs and then deletes logs that exceed the expiration period or quota size. *Weekly summary logs can age beyond the threshold before the next deletion if they reach the expiration threshold between times when the firewall deletes logs. When a log quota reaches the maximum size, new log entries start overwriting the oldest log entries. If you reduce a log quota size, the firewall or Panorama removes the oldest logs when you commit the changes. In an HA active/passive configuration, the passive peer does not receive logs and, therefore, does*

Item	Description
	not delete them unless failover occurs and the passive peer becomes active.

	• **Core Files**—If your firewall experiences a system process failure, it will generate a core file that contains details about the process and why it failed. If a core file is too large for the default core file storage location (`/var/cores` partition), you can enable the **`large-core`** file option to allocate an alternate and larger storage location (`/opt/panlogs/cores`). A Palo Alto Networks support engineer can increase the allocated storage if needed.
	To enable or disable the **`large-core`** file option, enter the following CLI command from configuration mode and then **`commit`** the configuration:
	`# set deviceconfig setting management large-core [yes|no]`
	The core file is deleted when you disable this option.
	You must use SCP from operational mode to export the core file:
	`> scp export core-file large-corefile`
	Only a Palo Alto Networks support engineer can interpret the contents of the core files.
	• **Restore Defaults**—Select this option to revert to the default values.

Session Log Storage and **Management Log Storage** tabs (PA-5200 Series and PA#7000 Series firewalls only)	PA-5200 Series and PA-7000 Series firewalls store management logs and session logs on separate disks. Select the tab for each set of logs and configure the settings described in Log Storage tab: • **Session Log Storage**—Select **Session Log Quota** and set the quotas and expiration periods for Traffic, Threat, URL Filtering, HIP Match, User-ID, GTP/Tunnel, SCTP, and Authentication logs, as well as Extended Threat PCAPs. • **Management Log Storage**—Set quotas and expiration periods for System, Config, and App Stats logs, as well as for HIP Reports, Data Filtering Captures, App PCAPs, and Debug Filter PCAPs.
Single Disk Storage and **Multi Disk Storage** tabs (Panorama template only)	If you use a Panorama template to configure log quotas and expiration periods, configure the settings in one or both of the following tabs based on the firewalls assigned to the template: • **PA-5200 Series and PA-7000 Series firewalls**—Select **Multi Disk Storage** and configure the settings in the Session Log Storage and Management Log Storage tabs.

Item	Description
	PA-5200 Series firewalls by default have a 0% quota allocated for SCTP log storage, SCTP Summary, Hourly SCTP Summary, Daily SCTP Summary, and Weekly SCTP Summary, so you must allocate some percentage for these firewalls to log SCTP information. • **All other firewall models**—Select **Single Disk Storage**, select **Session Log Quota**, and configure the settings on the Log Storage tab.
Log Export and Reporting tab	Configure the following log export and reporting settings as needed: • **Number of Versions for Config Audit**—Enter the number of configuration versions to save before discarding the oldest ones (default is 100). You can use these saved versions to audit and compare changes in configuration. • **Number of Versions for Config Backups**—(Panorama only) Enter the number of configuration backups to save before discarding the oldest ones (default is 100). • **Max Rows in CSV Export**—Enter the maximum number of rows that will appear in the CSV reports generated when you **Export to CSV** from the traffic logs view (range is 1 to 1,048,576; default is 65,535). • **Max Rows in User Activity Report**—Enter the maximum number of rows that is supported for the detailed user activity reports (range is 1 to 1,048,576; default is 5,000).
Log Export and Reporting tab (cont)	• **Average Browse Time (sec)**—Configure this variable to adjust how the browse time is calculated in seconds for the Monitor > PDF Reports > User Activity Report (range is 0 to 300 seconds; default is 60). The calculation will ignore sites categorized as web advertisements and content delivery networks. The browse time calculation is based on container pages logged in the URL filtering logs. Container pages are used as the basis for this calculation because many sites load content from external sites that should not be considered. For more information on the container page, see Container Pages. The average browse time setting is the average time that the administrator thinks it should take a user to browse a web page. Any request made after the average browse time has elapsed will be considered a new browsing activity. The calculation will ignore any new web pages that are loaded between the time of the first request (start time) and the average browse time. This behavior was designed to exclude any external sites that are loaded within the web page of interest. Example: If the average browse time setting is 2 minutes and a user opens a web page and views that page for 5 minutes, the browse time for that page will still be 2 minutes. This is done because there is no way to determine how long a user views a given page.

Item	Description
	• **Page Load Threshold (sec)**—Allows you to adjust the assumed time (in seconds) that it takes for page elements to load on the page (range is 0 to 60; default is 20). Any request that occurs between the first page load and the page load threshold is assumed to be elements of the page. Any requests that occur outside of the page load threshold is assumed to be the user clicking a link within the page. The page load threshold is also used in the calculations for the Monitor > PDF Reports > User Activity Report. • **Syslog HOSTNAME Format**—Select whether to use the FQDN, hostname, or IP address (IPv4 or IPv6) in the syslog message header. This header identifies the firewall or Panorama management server where the message originated. • **Report Runtime**—Select the time of day (default is 2 a.m.) when the firewall or Panorama appliance starts generating daily scheduled reports. • **Report Expiration Period**—Set the expiration period (in days) for reports (range is 1 to 2,000). By default, there is no expiration period, which means reports never expire. The firewall or Panorama appliance deletes expired reports nightly at 2 A.M. according to its system time.
	• **Stop Traffic when LogDb full** (Firewall only; disabled by default)—Select this option if you want traffic through the firewall to stop when the log database is full. • **Enable Threat Vault Access** (enabled by default)—Enables the firewall to access the Threat Vault to gather the latest information about detected threats. This information is available for threat logs and for top threat activity charted on the ACC. • **Enable Log on High DP Load** (Firewall only; disabled by default)—Select this option to specify that a system log entry is generated when the packet processing load on the firewall is at 100% CPU utilization.  *Enable Log on High DP Load allows administrators to investigate and identify the cause of high CPU utilization.* *A high CPU load can cause operational degradation because the CPU does not have enough cycles to process all packets. The system log alerts you to this issue (a log entry is generated each minute) and allows you to investigate for probable cause.* • **Enable High Speed Log Forwarding** (PA-5200 Series and PA-7000 Series firewalls only; disabled by default)—As a best practice, select this option to forward logs to Panorama at up to a maximum rate of 120,000 logs per second. When disabled, the firewall forwards logs to Panorama at a maximum rate of only 80,000 logs per second.

Item	Description
	If you enable this option, the firewall does not store logs locally or display them in the **Dashboard**, **ACC**, or **Monitor** tabs. Additionally, you must configure log forwarding to Panorama to use this option. • **Log Collector Status**—Displays status of whether the firewall successfully established a connection to the Distributed Log Collection architecture and is sending logs to it. If the firewall is also configured to send logs to the Logging Service, verify the **Logging Service Status**, in the Logging Service section.
(Panorama only)	• **Buffered Log Forwarding from Device** (enabled by default)—Allows the firewall to buffer log entries on its hard disk (local storage) when it loses connectivity to Panorama. When the connection to Panorama is restored, the firewall forwards the log entries to Panorama; the disk space available for buffering depends on the log storage quota for the firewall model and the volume of logs that are pending roll over. If the available space is consumed, the oldest entries are deleted to allow logging of new events. *Enable Buffered Log Forwarding from Device to help prevent loss of logs if the connection to Panorama goes down.* • **Get Only New Logs on Convert to Primary** (disabled by default)—This option applies only to a Panorama virtual appliance in Legacy mode that writes logs to a Network File System (NFS). With NFS logging, only the primary Panorama is mounted to the NFS. Therefore, the firewalls send logs only to the active primary Panorama. This option enables you to configure firewalls to send newly generated logs only to Panorama when an HA failover occurs and the secondary Panorama resumes logging to the NFS (after it is promoted as primary). This option is typically enabled to prevent firewalls from sending a large volume of buffered logs when connectivity to Panorama is restored after a significant period of time. • **Only Active Primary Logs to Local Disk** (disabled by default)—This option applies only to a Panorama virtual appliance in Legacy mode. This option enables you to configure only the active Panorama to save logs to the local disk.
	Pre-Defined Reports (enabled by default)—Pre-defined reports for application, traffic, threat, URL Filtering, and Stream Control Transmission Protocol (SCTP) are available on the firewall and on Panorama. Pre-defined reports for SCTP are available on the firewall and Panorama after SCTP Security is enabled in **Device** > **Setup** > **Management** > **General Settings**. Because the firewalls consume memory resources in generating the results hourly (and forwarding it to Panorama where it is aggregated and compiled for viewing), to reduce memory usage,

Item	Description
	you can disable the reports that are not relevant to you. To disable a report, disable this option for the report. Click **Select All** or **Deselect All** to entirely enable or disable the generation of pre-defined reports. *Before disabling a report, verify that there isn't a Group Report or a PDF Report using it. If you disable a pre-defined report assigned to a set of reports, the entire set of reports will have no data.*

Banners and Messages

To view all messages in a Message of the Day dialog, see Message of the Day.

After you configure the Message of the Day and click OK, administrators who subsequently log in and active administrators who refresh their browsers will see the new or updated message immediately; a commit is not required. This enables you to warn other administrators of an impending commit before you perform that commit.

Message of the Day (check box)	Select this option to enable the Message of the Day dialog to display when an administrator logs in to the web interface.
Message of the Day (text-entry field)	Enter the text (up to 3,200 characters) for the Message of the Day dialog.
Allow Do Not Display Again	Select this option (disabled by default) to include a **Do not show again** option in the Message of the Day dialog. This gives administrators the option to avoid seeing the same message in subsequent logins. *If you modify the Message of the Day text, the message displays even to administrators who selected Do not show again. Administrators must reselect this option to avoid seeing the modified message in subsequent sessions unless the message is modified again.*
Title	Enter text for the Message of the Day header (default is `Message of the Day`).
Background Color	Select a background color for the Message of the Day dialog. The default (**None**) is a light gray background.
Icon	Select a predefined icon to appear above the text in the Message of the Day dialog: • **None** (default) • **Error** • **Help**

Item	Description
	• **Information** • **Warning**
Header Banner	Enter the text that the header banner displays (up to 3,200 characters).
Header Color	Select a color for the header background. The default (**None**) is a transparent background.
Header Text Color	Select a color for the header text. The default (**None**) is black.
Same banner for header and footer	Select this option (enabled by default) if you want the footer banner to have the same text and colors as the header banner. When enabled, the fields for the footer banner text and colors are grayed out.
Footer Banner	Enter the text that the footer banner displays (up to 3,200 characters).
Footer Color	Select a color for the footer background. The default (**None**) is a transparent background.
Footer Text Color	Select a color for the footer text. The default (**None**) is black.
Minimum Password Complexity	
Enabled	Enable minimum password requirements for local accounts. With this feature, you can ensure that local administrator accounts on the firewall will adhere to a defined set of password requirements. You can also create a password profile with a subset of these options that will override these settings and can be applied to specific accounts. For more information, see Device > Password Profiles and see Username and Password Requirements for information on valid characters that can be used for accounts. *The maximum password length is 31 characters. Avoid setting requirements that PAN-OS does not accept. For example, do not set a requirement of 10 uppercase, 10 lower case, 10 numbers, and 10 special characters because that would exceed the maximum length of 31 characters.* If you have high availability (HA) configured, always use the primary peer when configuring password complexity options and commit soon after making changes. Minimum password complexity settings do not apply to local database accounts for which you specified a **Password Hash** (see Device > Local User Database > Users).

Item	Description
	 *Require strong passwords to help prevent brute force network access attacks from succeeding. Require a minimum length and the use of at least one each of uppercase letters, lowercase letters, numerical values, and special characters. In addition, prevent excessive repetition of characters and usernames in passwords, set limits on how often passwords can be reused, and set regular password change periods so passwords don't stay in use too long. The stronger the password requirements, the more difficult you make it for attackers to hack a password. Be sure to use the* best practices for password strength *to ensure a strict password.*
Minimum Length	Require a minimum password length (range is 1 to 15 characters).
Minimum Uppercase Letters	Require a minimum number of uppercase letters (ranges is 0 to 15 characters).
Minimum Lowercase Letters	Require a minimum number of lowercase letters (range is 0 to 15 characters).
Minimum Numeric Letters	Require a minimum number of numeric letters (range is 0 to 15 numbers).
Minimum Special Characters	Require a minimum number of special (non-alphanumeric) characters (range is 0 to 15 characters).
Block Repeated Characters	Specify the number of sequential duplicate characters permitted in a password (range is 2 to 15). If you set the value to 2, the password can contain the same character in sequence twice but if the same character is used three or more times in sequence, the password is not permitted. For example, if the value is set to 2, the system will accept the password test11 or 11test11, but not test111, because the number 1 appears three times in sequence.
Block Username Inclusion (including reversed)	Select this option to prevent the account username (or reversed version of the name) from being used in the password.
New Password Differs By Characters	When administrators change their passwords, the characters must differ by the specified value.
Require Password Change on First Login	Select this option to prompt administrators to change their passwords the first time they log in to the firewall.
Prevent Password Reuse Limit	Require that a previous password is not reused based on the specified count. For example, if the value is set to 4, you could not reuse any of your last 4 passwords (range is 0 to 50).

Item	Description
Block Password Change Period (days)	User cannot change their passwords until the specified number of days is reached (range is 0 to 365 days).
Required Password Change Period (days)	Require that administrators change their password on a regular basis (in days) (range is 0 to 365). For example, if the value is set to 90, administrators are prompted to change their password every 90 days. You can also set an expiration warning from 0 to 30 days and specify a grace period.
Expiration Warning Period (days)	If a **Required Password Change Period** is set, you can use this **Expiration Warning Period** to prompt users at each log in to change their password when there are less than a specified number of days remaining before the required change date (range is 0 to 30).
Post Expiration Admin Login Count (count)	Allow the administrator to log in a specified number of times after the required change date (range is 0 to 3). For example, if you set this value to 3 and their account has expired, they can log in 3 more times without changing their password before their account is locked out.
Post Expiration Grace Period (days)	Allow the administrator to log in for a specified number of days after the account has expired (range is 0 to 30).
AutoFocus™	
Enabled	Enable the firewall to connect to an AutoFocus portal to retrieve threat intelligence data and to enable integrated searches between the firewall and AutoFocus. When connected to AutoFocus, the firewall displays AutoFocus data associated with Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering log entries (**Monitor** > **Logs**). You can click on an artifact in these types of log entries (such as an IP address or a URL) to display a summary of the AutoFocus findings and statistics for that artifact. You can then open an expanded AutoFocus search for the artifact directly from the firewall. *Check that your AutoFocus license is active on the firewall (Device > Licenses). If the AutoFocus license is not displayed, use one of the License Management options to activate the license.*
AutoFocus URL	Enter the AutoFocus URL: **`https://autofocus.paloaltonetworks.com:10443`**
Query Timeout (sec)	Set the duration of time (in seconds) for the firewall to attempt to query AutoFocus for threat intelligence data. If the AutoFocus

Item	Description
	portal does not respond before the end of the specified period, the firewall closes the connection.

Cortex Data Lake

Use this section to configure VM-Series and hardware-based firewalls to forward logs to Cortex Data Lake. Here's the full workflow to configure the options described below:

- Start Logging to Cortex Data Lake (without Panorama)
- Start Logging to Cortex Data Lake (for Panorama-managed firewalls)

The Logging Service is now called Cortex Data Lake; however, some firewall features and buttons still display the Logging Service name.

Enable Cortex Data Lake	Pick this option to enable the firewall (or, if you're using Panorama, firewalls that belong to the selected **Template**) to forward logs to Cortex Data Lake (Cortex Data Lake was previously called the Logging Service). After you configure Log Forwarding (Objects > Log Forwarding), the firewall forwards logs directly to Cortex Data Lake—this is true even for Panorama-managed firewalls.
Enable Duplicate Logging (for Panorama-managed firewalls only)	**Enable Duplicate Logging** to continue to send logs to Panorama and distributed Log Collectors, in addition to sending logs to Cortex Data Lake. This is a helpful option if you're evaluating Cortex Data Lake—when enabled, the firewalls that belong to the selected Template will save a copy of the logs to Cortex Data Lake and to your Panorama or Distributed Log Collection architecture.
Enable Enhanced Application Logging	**Enable Enhanced Application Logging** if you want the firewall to collect data that increases network visibility for Palo Alto Networks applications. For example, this increased network visibility enables Palo Alto Networks Cortex XDR apps to better categorize and establish a baseline for normal network activity so that the firewall can detect unusual behavior that might indicate an attack. Enhanced Application Logging requires a Logging Service (Cortex Data Lake) license. You cannot view these logs—they are designed to be consumed only by Palo Alto Networks applications.
Region	Select the geographic region of the Cortex Data Lake (Logging Service) instance to which the firewall will forward logs. Log in to the Cortex hub to confirm the region in which a Cortex Data Lake instance is deployed (in the hub, select the settings gear on the top menu bar and **Manage Apps**).
Connection count to Cortex Data Lake for PA-7000 Series and PA-5200 Series Firewalls	(PA-7000 Series and PA-5200 Series firewalls only) Specify the number of connections for sending logs from the firewalls to Cortex Data Lake (range is 1 to 20; default is 5). You can use the **`request logging-service-forwarding status`**

Item	Description
	CLI command on the firewall to verify the number of active connections between the firewall and Cortex Data Lake.
Onboard without Panorama (for firewalls that are not managed by Panorama)	You can enable firewalls that are not managed by Panorama to send logs to Cortex Data Lake. To do this, you need to first generate a key in the Cortex Data Lake app. This key enables the firewall to authenticate and securely connect to Cortex Data Lake. After you generate the key, enter it and enable the firewall to start forwarding logs to Cortex Data Lake.
Logging Service Status	View the status of the connection to Cortex Data Lake. **Show Status** to view the details for the following checks: • **License**—`OK` or `Error` to indicate whether the firewall has a valid license to forward logs to Cortex Data Lake. • **Certificate**—`OK` or `Error` to indicate whether the firewall successfully fetched the certificate required to authenticate to Cortex Data Lake. • **Customer Info**—`OK` or `Error` to indicate whether the firewall has the required customer identification number to use Cortex Data Lake. When the status is `OK`, you can see the customer identification number as well. • **Device Connectivity**—Indicates whether the firewall is successfully connected to Cortex Data Lake.
SSH Management Profiles Settings	
Server Profile	A type of SSH service profile that applies to the SSH sessions for the CLI management connections on your network. To apply an existing server profile, select a profile, click **OK**, and **Commit** your change. *You must perform an SSH service restart from your CLI to activate the profile.* For more information, see Device > Certificate Management > SSH Service Profile.

Device > Setup > Operations

You can perform the following tasks to manage the running and candidate configurations of the firewall and Panorama™. If you're using a Panorama virtual appliance, you can also use the settings on this page to configure Log Storage Partitions for a Panorama Virtual Appliance in Legacy Mode.

You must Commit Changes *you make in the candidate configuration to activate those changes at which point they become part of the running configuration. As a best practice, periodically* Save Candidate Configurations*.*

You can use Secure Copy (SCP) commands from the CLI *to export configuration files, logs, reports, and other files to an SCP server and import the files to another firewall or Panorama M-Series or virtual appliance. However, because the log database is too large for an export or import to be practical, the following models do not support export or import of the entire log database: PA-7000 Series firewalls (all PAN-OS® releases), Panorama virtual appliances running Panorama 6.0 or later releases, and Panorama M-Series appliances (all Panorama releases).*

Function	Description
Configuration Management	
Revert to last saved configuration	Restores the default snapshot (.snapshot.xml) of the candidate configuration (the snapshot that you create or overwrite when you select **Config** > **Save Changes** at the top right of the web interface). (Panorama only) **Select Device Groups & Templates** to select specific device groups, templates, or template stacks configurations to revert. Device Group and Template Admins can only select the device groups, templates, or template stacks designated in their assigned access domain.
Revert to running config	Restores the current running configuration. This operation undoes all changes that every administrator made to the candidate configuration since the last commit. To revert only the changes of specific administrators, see Revert Changes. (Panorama only) **Select Device Groups & Templates** to select specific device groups, templates, or template stacks configurations to revert. Device Group and Template Admins can only select the device groups, templates, or template stacks designated in their assigned access domain.
Save named configuration snapshot	Creates a candidate configuration snapshot that does not overwrite the default snapshot (.snapshot.xml). Enter a **Name** for the snapshot or select an existing named snapshot to overwrite. (Panorama only) **Select Device Groups & Templates** to select specific device groups, templates, or template stacks configurations to save. Device Group and Template Admins can only select the device groups, templates, or template stacks designated in their assigned access domain.
Save candidate config	Creates or overwrites the default snapshot of the candidate configuration (.snapshot.xml) with the current candidate configuration. This is the same action as when you select **Config** > **Save Changes** at the top right of the

Function	Description
	web interface. To save only the changes of specific administrators, see Save Candidate Configurations. (Panorama only) **Select Device Groups & Templates** to select specific device groups, templates, or template stacks configurations to save. Device Group and Template Admins can only select the device groups, templates, or template stacks designated in their assigned access domain.
Load named configuration snapshot (firewall) or Load named Panorama configuration snapshot	Overwrites the current candidate configuration with one of the following: • Custom-named candidate configuration snapshot (instead of the default snapshot). • Custom-named running configuration that you imported. • Current running configuration. The configuration must reside on the firewall or Panorama onto which you are loading it. Select the **Name** of the configuration and enter the **Decryption Key**, which is the master key of the firewall or Panorama (see Device > Master Key and Diagnostics). The master key is required to decrypt all the passwords and private keys within the configuration. If you are loading an imported configuration, you must enter the master key of the firewall or Panorama from which you imported. After the load operation finishes, the master key of the firewall or Panorama onto which you loaded the configuration re-encrypts the passwords and private keys. To generate new UUIDs for all rules in the configuration (for example, if you are loading a configuration from another firewall but you want to maintain unique rules when you load that configuration), the superuser must **Regenerate Rule UUIDs for selected named configuration** to generate new UUIDs for all rules. (Panorama only) Specify object, policy, device group, or template configurations to partially load configurations from the named configuration by selecting from the following: • **Load Shared Objects**—Load only the Shared objects, along with all device group and template configurations. • **Load Shared Policies**—Load only the Shared policies, along with all device group and template configurations. • **Select Device Groups & Templates**—Specify device groups, templates, or template stacks configurations to load. Device Group and Template Admins can only select the device groups, templates, or template stacks designated in their assigned access domain • **Retain Rule UUIDs**—Keep the UUIDs in the current running configuration.
Load configuration version (firewall) or Load Panorama configuration version	Overwrites the current candidate configuration with a previous version of the running configuration that is stored on the firewall or Panorama. Select the **Name** of the configuration and enter the **Decryption Key**, which is the master key of the firewall or Panorama (see Device > Master Key and Diagnostics). The master key is required to decrypt all the passwords and private keys within the configuration. After the load operation finishes, the master key re-encrypts the passwords and private keys.

Function	Description
	(Panorama only) Specify object, policy, device group or template configurations to partially load configurations from the named configuration by selecting: • **Load Shared Objects**—Load only the Shared objects, along with all device group and template configurations. • **Load Shared Policies**—Load only the Shared policies, along with all device group and template configurations. • **Select Device Groups & Templates**—Specify device groups, templates, or template stacks configurations to load. Device Group and Template Admins can only select the device groups, templates, or template stacks designated in their assigned access domain
Export named configuration snapshot	Exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. (Panorama only) **Select Device Groups & Templates** to select specific device groups, templates, or template stacks configurations to export. Device Group and Template Admins can only select the device groups, templates, or template stacks designated in their assigned access domain.
Export configuration version	Exports a **Version** of the running configuration as an XML file. (Panorama only) **Select Device Groups & Templates** to select specific device groups, templates, or template stacks configurations to export. Device Group and Template Admins can only select the device groups, templates, or template stacks designated in their assigned access domain.
Export Panorama and devices config bundle (Panorama only)	Generates and exports the latest versions of the Panorama running configuration backup and of each managed firewall. To automate the process of creating and exporting the configuration bundle daily to an SCP or FTP server, see Panorama > Device Deployment.
Export or push device config bundle (Panorama only)	Prompts you to select a firewall and perform one of the following actions on the firewall configuration stored on Panorama: • **Push & Commit** the configuration to the firewall. This action cleans the firewall (removes any local configuration from it) and pushes the firewall configuration stored on Panorama. After you import a firewall configuration, use this option to clean that firewall so you can manage it using Panorama. • **Export** the configuration to the firewall without loading it. To load the configuration, you must access the firewall CLI and run the configuration mode command **load device-state**. This command cleans the firewall in the same way as the **Push & Commit** option. *These options are available only for firewalls running PAN-OS 6.0.4 and later releases.*
Export device state (Firewall only)	Exports the firewall state information as a bundle. In addition to the running configuration, the state information includes device group and template settings pushed from Panorama. If the firewall is a GlobalProtect™ portal,

Function	Description
	the bundle also includes certificate information, a list of satellites that the portal manages, and satellite authentication information. If you replace a firewall or portal, you can restore the exported information on the replacement by importing the state bundle. *You must manually run the firewall state export or create a scheduled XML API script to export the file to a remote server. This should be done on a regular basis because satellite certificates often change.* To create the firewall state file from the CLI, from configuration mode, run the **`save device state`** command. The file will be named `device_state_cfg.tgz` and is stored in `/opt/pancfg/mgmt/device-state`. The operational command to export the firewall state file is **`scp export device-state`** (you can also use **`tftp export device-state`**). For information on using the XML or REST API, refer to the PAN-OS and Panorama API Guide.
Import named config snapshot	Imports a running or candidate configuration from any network location. Click **Browse** and select the configuration file to be imported.
Import device state (Firewall only)	Imports the state information bundle you exported from a firewall when you chose to **Export device state**. Besides the running configuration, the state information includes device group and template settings pushed from Panorama. If the firewall is a GlobalProtect portal, the bundle also includes certificate information, a list of satellites, and satellite authentication information. If you replace a firewall or portal, you can restore the information on the replacement by importing the state bundle.
Import Device Configuration to Panorama (Panorama only)	Imports a firewall configuration into Panorama. Panorama automatically creates a template to contain the network and device configurations. For each virtual system (vsys) on the firewall, Panorama automatically creates a device group to contain the policy and object configurations. The device groups will be one level below the Shared location in the hierarchy, though you can reassign them to a different parent device group after finishing the import (see Panorama > VMware NSX). *The content versions on Panorama (for example, Applications and Threats database) must be the same as or higher than the versions on the firewall from which you will import a configuration.* Configure the following import options: • **Device**—Select the firewall from which Panorama will import the configurations. The drop-down includes only firewalls that are connected to Panorama and are not assigned to any device group or template. You can select only an entire firewall, not an individual vsys. • **Template Name**—Enter a name for the template that will contain the imported device and network settings. For a multi-vsys firewall, the field is blank. For other firewalls, the default value is the firewall name. You cannot use the name of an existing template.

Function	Description
	• **Device Group Name Prefix** (multi-vsys firewalls only)—Optionally, add a character string as a prefix for each device group name. • **Device Group Name**—For a multi-vsys firewall, each device group has a vsys name by default. For a other firewalls, the default value is the firewall name. You can edit the default names but cannot use the name of an existing device group. • **Import devices' shared objects into Panorama's shared context** (enabled by default)—Panorama imports objects that belong to Shared in the firewall to Shared in Panorama.  *Panorama regards all objects as shared on a firewall without multiple virtual systems. If you disable this option, Panorama copies shared firewall objects into device groups instead of Shared. This setting has the following exceptions:* • If a shared firewall object has the same name and value as an existing shared Panorama object, the import excludes that firewall object. • If the name or value of the shared firewall object differs from the shared Panorama object, Panorama imports the firewall object into each device group. • If a configuration imported into a template references a shared firewall object, Panorama imports that object into Shared regardless of whether you select this option. • If a shared firewall object references a configuration imported into a template, Panorama imports the object into a device group regardless of whether you select this option. • **Rule Import Location**—Select whether Panorama will import policies as pre-rules or post-rules. Regardless of your selection, Panorama imports default security rules (intrazone-default and interzone-default) into the post-rulebase.  *If Panorama has a rule with the same name as a firewall rule that you import, Panorama displays both rules. However, rule names must be unique: delete one of the rules before performing a commit on Panorama or the commit will fail.*
Device Operations	
Reboot	To restart the firewall or Panorama, **Reboot Device**. The firewall or Panorama logs you out, reloads the software (PAN-OS or Panorama) and the active configuration, closes and logs existing sessions, and creates a System log entry that shows the name of the administrator who initiated the shutdown. Any configuration changes that were not saved or committed are lost (see Device > Setup > Operations).  *If the web interface is not available, use the following operational CLI command:* `request restart system`

Function	Description
Shutdown	To perform a graceful shutdown of the firewall or Panorama, **Shutdown Device** or **Shutdown Panorama** and then click **Yes** when prompted. Any configuration changes that are not saved or committed are lost. All administrators will be logged off and the following processes will occur: • All login sessions will be logged off. • Interfaces will be disabled. • All system processes will be stopped. • Existing sessions will be closed and logged. • System Logs will be created that will show the administrator name who initiated the shutdown. If this log entry cannot be written, a warning will appear and the system will not shutdown. • Disk drives will be cleanly unmounted and the firewall or Panorama will power off. You must unplug the power source and plug it back in before you can power back on the firewall or Panorama.  *If the web interface is not available, use the following CLI command:* **`request shutdown system`**
Restart Dataplane	**Restart Dataplane** to restart the data functions of the firewall without rebooting. This option is not available on Panorama or PA-220, PA-800 Series, or VM-Series firewalls.  *If the web interface is not available, use the following CLI command:* ***`request restart dataplane`*** On a PA-7000 Series firewall, each NPC has a dataplane so you can restart the NPC to perform this operation by running the command **`request chassis restart slot`**.
Miscellaneous	
Custom Logos	Use **Custom Logos** to customize any of the following: • **Login Screen** background image • **Main UI** (web interface) header image • **PDF Report Title Page** image. Refer to Monitor > PDF Reports > Manage PDF Summary. • **PDF Report Footer** image Upload (<image>) an image file to preview it or delete ( ) a previously-uploaded image. To return to the default logo, remove your entry and **Commit**. For the **Login Screen** and **Main UI**, you can display ( ) the image as it will appear; if necessary, the firewall crops the image to fit. For PDF reports, the

Function	Description
	firewall automatically resizes the images to fit without cropping. In all cases, the preview displays the recommended image dimensions. The maximum image size for any logo is 128KB. The supported file types are .png, .gif, and .jpg. The firewall does not support image files that are interlaced or that contain alpha channels because such files interfere with PDF report generation. You might need to contact the illustrator who created an image to remove alpha channels or make sure the graphics software you are using does not save files with the alpha channel feature. For information on generating PDF reports, see Monitor > PDF Reports > Manage PDF Summary.
SNMP Setup	Enable SNMP Monitoring.
Storage Partition Setup (Panorama only)	Log Storage Partitions for a Panorama Virtual Appliance in Legacy Mode.

Enable SNMP Monitoring

- Device > Setup > Operations

Simple Network Management Protocol (SNMP) is a standard protocol for monitoring the devices on your network. Select **Operations** to configure the firewall to use the SNMP version that your SNMP manager supports (SNMPv2c or SNMPv3). For a list of the MIBs that you must load into the SNMP manager so it can interpret the statistics it collects from the firewall, see Supported MIBs. To configure the server profile that enables the firewall to communicate with the SNMP trap destinations on your network, see Device > Server Profiles > SNMP Trap. The SNMP MIBs define all SNMP traps that the firewall generates. An SNMP trap identifies an event with a unique Object ID (OID) and the individual fields are defined as a variable binding (varbind) list. Click **SNMP Setup** and specify the following settings to allow SNMP GET requests from your SNMP manager:

Field	Description
Physical Location	Specify the physical location of the firewall. When a log or trap is generated, this information allows you to identify (in an SNMP manager) the firewall that generated the notification.
Contact	Enter the name or email address of the person responsible for maintaining the firewall. This setting is reported in the standard system information MIB.
Use Specific Trap Definitions	This option is selected by default, which means the firewall uses a unique OID for each SNMP trap based on the event type. If you clear this option, every trap will have the same OID.
Version	Select the SNMP version: **V2c** (default) or **V3**. Your selection controls the remaining fields that the dialog displays.
For SNMP V2c	
SNMP Community String	Enter the community string, which identifies an SNMP *community* of SNMP managers and monitored devices and also serves as a password to

Field	Description
	authenticate the community members to each other when they exchange SNMP get (statistics request) and trap messages. The string can have up to 127 characters, accepts all characters, and is case-sensitive.  *Don't use the default community string public. Because SNMP messages contain community strings in clear text, consider the security requirements of your network when defining community membership (administrator access).*
For SNMP V3	
Name / View	You can assign a group of one or more views to the user of an SNMP manager to control which MIB objects (statistics) the user can get from the firewall. Each view is a paired OID and bitwise mask: the OID specifies a MIB and the mask (in hexadecimal format) specifies which objects are accessible within (include matching) or outside (exclude matching) that MIB. For example, if the **OID** is 1.3.6.1, the matching **Option** is set to **include** and the **Mask** is 0xf0, then the objects that the user requests must have OIDs that match the first four nodes (f = 1111) of 1.3.6.1. The objects don't need to match the remaining nodes. In this example, 1.3.6.1.2 matches the mask and 1.4.6.1.2 doesn't. For each group of views, click **Add**, enter a **Name** for the group, and then configure the following for each view you **Add** to the group: • **View**—Specify a name for the view. The name can have up to 31 characters that are alphanumeric, periods, underscores, or hyphens. • **OID**—Specify the OID of the MIB. • **Option**—Select the matching logic to apply to the MIB. • **Mask**—Specify the mask in hexadecimal format.  *To provide access to all management information, use the top-level OID 1.3.6.1, set the Mask to 0xf0, and set the matching Option to include.*
Users	SNMP user accounts provide authentication, privacy, and access control when firewalls forward traps and SNMP managers get firewall statistics. For each user, click **Add** and configure the following settings: • **Users**—Specify a username to identify the SNMP user account. The username you configure on the firewall must match the username configured on the SNMP manager. The username can have up to 31 characters. • **View**—Assign a group of views to the user. • **Auth Password**—Specify the authentication password of the user. The firewall uses the password to authenticate to the SNMP manager when forwarding traps and responding to statistics requests. The firewall uses Secure Hash Algorithm (SHA-1 160) to encrypt the password. The password must be 8-256 characters and all characters are allowed. • **Priv Password**—Specify the privacy password of the user. The firewall uses the password and Advanced Encryption Standard (AES-128) to encrypt

Field	Description
	SNMP traps and responses to statistics requests. The password must be 8-256 characters and all characters are allowed.

Device > Setup > HSM

Select **Device** > **Setup** > **HSM** to configure a Hardware Security Module (HSM), perform operations, and view HSM status.

What are you looking for?	See:
What is the purpose of a Hardware Security Module (HSM) and where can I find detailed configuration procedures?	Secure Keys with a Hardware Security Module
Configure:	Hardware Security Module Provider Settings
	HSM Authentication
Perform Hardware Security Operations	Hardware Security Operations
How do I view HSM status?	Hardware Security Module Provider Configuration and Status
	Hardware Security Module Status

Hardware Security Module Provider Settings

To configure a Hardware Security Module (HSM) on the firewall, edit the Hardware Security Module Provider settings:

Hardware Security Module Provider Settings	Description
Provider Configured	Select the HSM vendor: • **None** (default)—The firewall does not connect to any HSM. • **SafeNet Network HSM** • **nCipher nShield Connect** *The HSM server version must be compatible with the HSM client version on the firewall.*
Module Name	Add a module name for the HSM. This can be any ASCII string up to 31 characters long. Add up to 16 module names if you are configuring independent or high availability SafeNet HSM configurations.
Server Address	Specify an IPv4 address for any HSM module you are configuring.
High Availability (SafeNet Network only)	(Optional) Select this option if you are configuring the SafeNet HSM modules in a high availability configuration. You must configure the module name and server address of each HSM module.

Hardware Security Module Provider Settings	Description
Auto Recovery Retry (SafeNet Network only)	Specify the number of times that the firewall will try to recover its connection to an HSM before failing over to another HSM in an HSM HA configuration (range is 0—500; default is 0).
High Availability Group Name (SafeNet Network only)	Specify a group name to be used for the HSM HA group. This name is used internally by the firewall. It can be any ASCII string up to 31 characters long.
Remove Filesystem Address (nCipher nShield Connect only)	Configure the IPv4 address of the remote file system used in the nShield Connect HSM configuration.

HSM Authentication

Select **Setup Hardware Security Module** and configure the following settings to authenticate the firewall to the HSM.

HSM Module Authentication	
Server Name	Select an HSM server name from the drop-down, then select if you want to authenticate and establish trust using automatic or manually generated certificates. • **Automatic** • **Manual** If you select **Manual**, you need to import and install the HSM server manually generated certificate. Export the HSM client certificate to install on the HSM server.
Administrator Password	Enter the administrator password of the HSM to authenticate the firewall to the HSM.

Hardware Security Operations

To perform an operation on the Hardware Security Module (HSM) or the firewall connected to the HSM, select **Device** > **Setup** > **HSM** and select one of the following Hardware Security Operations:

Hardware Security Operations	
Setup Hardware Security Module	Configures the firewall to authenticate with an HSM.
Show Detailed Information	Displays information about HSM servers, HSM high availability status, and HSM hardware.

Hardware Security Operations	
Synchronize with Remote Filesystem (nCipher nShield Connect only)	Synchronizes the key data from the nShield Connect remote file system to the firewall.
Reset Configuration	Removes all HSM connections to the firewall. You must repeat all authentication procedures after resetting the HSM configuration.
Select HSM Client Version (SafeNet Network only)	Allows you to choose the version of software running on the HSM client (the firewall). The HSM client version must be compatible with the HSM server version. See the HSM vendor documentation for a matrix of client-server version compatibility.

Hardware Security Module Provider Configuration and Status

The Hardware Security Module Provider section shows the HSM configuration settings and the connectivity status of the HSM.

Hardware Security Module Provider Status	
Provider Configured	Select the HSM vendor configured on the firewall: • **None** • **SafeNet Network HSM** • **nCipher nShield Connect**
High Availability	(SafeNet Network only) HSM high availability is configured if checked.
High Availability Group Name	(SafeNet Network only) The group name configured on the firewall for HSM high availability.
Remote Filesystem Address	(nShield Connect only) The address of the remote filesystem.
Firewall Source Address	The address of the port used for the HSM service. By default this is the management port address. It can be specified as a different port however through the Services Route Configuration in **Device** > **Setup** > **Services**.
HSM Client Version on Firewall	Shows the HSM client version installed.
Master Key Secured by HSM	If checked, the master key is secured on the HSM.
Status	Shows green if the firewall is connected and authenticated to the HSM and shows red if the firewall is not authenticated or if network connectivity to the HSM is down. You can also Hardware Security Module Status for more details on the HSM connection.

Hardware Security Module Status

The Hardware Security Module Status includes the following information about HSMs that have been successfully authenticated. The display is different depending on the HSM provider configured (SafeNet or nCipher).

Hardware Security Module Status	
SafeNet Network HSM	• **Serial Number**—The serial number of the HSM partition is displayed if the HSM partition has successfully authenticated. • **Partition**—The partition name on the HSM that was assigned on the firewall. • **Module State**—The current operating state of the HSM connection. This field shows **Authenticated** if the HSM is displayed in this table.
nCipher nShield Connect HSM	• **Name**—The Server name of the HSM. • **IP address**—The IP address of the HSM that was assigned on the firewall. • **Module State**—The current operating state of the HSM connection. This setting shows **Authenticated** if the firewall successfully authenticated to the HSM and shows **Not Authenticated** if authentication failed.

Device > Setup > Services

The following topics describe global and virtual systems services settings on the firewall:

- Configure Services for Global and Virtual Systems
- Global Services Settings
- IPv4 and IPv6 Support for Service Route Configuration
- Destination Service Route

Configure Services for Global and Virtual Systems

On a firewall where multiple virtual systems are enabled, select **Services** to display the **Global** and **Virtual Systems** tabs where you set services that the firewall or its virtual systems, respectively, use to operate efficiently. (If the firewall is a single virtual system or if multiple virtual systems are disabled, the **Virtual Systems** tab is not shown.)

Select **Global** to set services for the whole firewall. These settings are also used as the default values for virtual systems that do not have a customized setting for a service.

- Edit **Services** to define the destination IP addresses of DNS servers, the Update Server, and the Proxy Server. Use the dedicated **NTP** tab to configure Network Time Protocol settings. See Table 12 for field descriptions of the available Services options.
- In **Service Features**, click **Service Route Configuration** to specify how the firewall will communicate with other servers/devices for services such as DNS, email, LDAP, RADIUS, syslog, and many more. There are two ways to configure global service routes:
  - The **Use Management Interface for all** option will force all firewall service communications with external servers through the management interface (MGT). If you select this option, you must configure the MGT interface to allow communications between the firewall and the servers/devices that provide services. To configure the MGT interface, select Device > Setup > Management and edit the settings.
  - The **Customize** option allows you granular control over service communication by configuring a specific source interface and IP address that the service will use as the destination interface and destination IP address in its response. (For example, you could configure a specific source IP/interface for all email communication between the firewall and an email server, and use a different source IP/interface for Palo Alto Networks Services.) Select the one or more services you want to customize to have the same settings and click **Set Selected Service Routes**. The services are listed in Table 13, which indicates whether a service can be configured for the **Global** firewall or **Virtual Systems**, and whether the service supports an IPv4 and/or IPv6 source address.

The **Destination** tab is another Global service route feature that you can customize. This tab appears in the Service Route Configuration window and is described in Destination Service Route.

Use the **Virtual Systems** tab to specify service routes for a single virtual system. Select a Location (virtual system) and click **Service Route Configuration**. Select **Inherit Global Service Route Configuration** or **Customize** service routes for a virtual system. If you choose to customize settings, select **IPv4** or **IPv6**. Select the one or more services you want to customize to have the same settings and click **Set Selected Service Routes**. See Table 13 for services that can be customized.

To control and redirect DNS queries between shared and specific virtual systems, you can use a DNS proxy and a DNS Server profile.

Global Services Settings

- Device > Setup > Services

To control and redirect DNS queries between shared and specific virtual systems, you can use a DNS proxy and a DNS Server profile.

Global Services Settings	Description
Services	
Update Server	Represents the IP address or host name of the server from which to download updates from Palo Alto Networks. The current value is **updates.paloaltonetworks.com**. Do not change this setting unless instructed by technical support.
Verify Update Server Identity	If you enable this option, the firewall or Panorama will verify that the server from which the software or content package is download has an SSL certificate signed by a trusted authority. This adds an additional level of security for the communication between firewalls or Panorama servers and the update server.  *Verify the update server identity to validate that the server has an SSL certificate signed by a trusted authority.*
DNS Settings	Choose the type of DNS service—**Servers** or **DNS Proxy Object**—for all DNS queries that the firewall initiates in support of FQDN address objects, logging, and firewall management. Options include: • Primary and secondary DNS servers to provide domain name resolution. • A DNS proxy configured on the firewall as an alternative to configuring DNS servers. If you enable a DNS proxy, you must enable **Cache** and **EDNS Cache Responses** (**Network** > **DNS Proxy** > **Advanced**).
Primary DNS Server	Enter the IP address of the primary DNS server for DNS queries from the firewall. For example, to find the update server, to resolve DNS entries in logs, or resolve FDQN-based address objects.
Secondary DNS Server	(Optional) Enter the IP address of a secondary DNS server to use if the primary server is unavailable.
Minimum FQDN Refresh Time (sec)	Set a limit on how fast the firewall refreshes FQDNs that it receives from a DNS. The firewall refreshes an FQDN based on the TTL of the FQDN as long as the TTL is greater than or equal to this **Minimum FQDN Refresh Time** (in seconds). If the TTL is less than this Minimum FQDN Refresh Time, the firewall refreshes the FQDN based on this Minimum FQDN Refresh Time (that is, the firewall does not honor TTLs faster than this setting). The timer starts when the firewall receives a DNS response from the DNS server or DNS proxy object resolving the FQDN (range is 0 to 14,400; default is 30). A setting of 0 means the firewall will refresh the FQDN based on the TTL value in the DNS and does not enforce a minimum FQDN refresh time.  *If the TTL for the FQDN in the DNS is short, but FQDN resolutions don't change as frequently as the TTL timeframe so don't require a faster refresh, you should set a minimum FQDN Refresh Time to avoid unnecessary FQDN refresh attempts.*

Global Services Settings	Description
FQDN Stale Entry Timeout (min)	Specify the length of time (in minutes) that the firewall continues to use stale FQDN resolutions in the event of a network failure or unreachable DNS server —when an FQDN is not getting refreshed (range is 0 to 10,080; default is 1,440). A value of 0 means the firewall does not continue to use a stale entry. If the DNS server is still unreachable at the end of the state timeout, the FQDN entry becomes unresolved (stale resolutions are removed).  *Make sure the FQDN Stale Entry Timeout value is short enough to not allow incorrect traffic forwarding (which poses a security risk), but is long enough to allow traffic continuity without causing an unplanned network outage.*
Proxy Server section	
Server	If the firewall needs to use a proxy server to reach Palo Alto Networks update services, enter the IP address or host name of the proxy server.
Port	Enter the port for the proxy server.
User	Enter the username for the administrator to enter when accessing the proxy server.
Password/ Confirm Password	Enter and confirm the password for the administrator to enter when accessing the proxy server.
Use proxy to send logs to Cortex Data Lake	Enable the firewall to send logs to Cortex Data Lake through the proxy server.
NTP	
NTP Server Address	Enter the IP address or hostname of an NTP server that you will use to synchronize the clock on the firewall. Optionally, you can enter the IP address or hostname of a second NTP server to synchronize the clock on the firewall if the primary server becomes unavailable.  *When an NTP server keeps all network firewall clocks synchronized, scheduled jobs run as expected and timestamps can help identify the root causes of issues that involve multiple devices. Configure a primary and a secondary NTP server in case the primary NTP server becomes unreachable.*
Authentication Type	You can enable the firewall to authenticate time updates from an NTP server. For each NTP server, select the type of authentication for the firewall to use: • **None** (default)—Select this option to disable NTP Authentication. • **Symmetric Key**—Select this option for the firewall to use symmetric key exchange (shared secrets) to authenticate time updates from the NTP server. If you select Symmetric Key, continue by specifying the following values: • **Key ID**—Enter the Key ID (1–65534).

Global Services Settings	Description
	• **Algorithm**—Select the MD5 or SHA1 algorithm to use for NTP authentication. • **Authentication Key/Confirm Authentication Key**—Enter and confirm the authentication key for the authentication algorithm. • **Autokey**—Select this option for the firewall to use autokey (public key cryptography) to authenticate time updates from the NTP server.  *Enable NTP server authentication so that the NTP server approves the client and provides synchronized updates.*

IPv4 and IPv6 Support for Service Route Configuration

The following table shows IPv4 and IPv6 support for service route configurations on global and virtual systems.

Service Route Configuration Settings	Global		Virtual System	
	IPv4	IPv6	IPv4	IPv6
AutoFocus—AutoFocus™ server.	✓	–	–	–
CRL Status—Certificate revocation list (CRL) server.	✓	✓	–	–
DDNS—Dynamic DNS service.	✓	✓	✓	✓
Panorama pushed updates—Content and software updates deployed from Panorama™.	✓	✓	–	–
DNS—Domain Name System server. *For virtual systems, DNS is done in the DNS Server Profile.	✓	✓	✓*	✓*
External Dynamic Lists—Updates for external dynamic lists.	✓	✓	–	–
Email—Email server.	✓	✓	✓	✓
HSM—Hardware security module server.	✓	–	–	✓
HTTP—HTTP forwarding.	✓	✓	✓	✓
Kerberos—Kerberos authentication server.	✓	–	✓	✓
LDAP—Lightweight Directory Access Protocol server.	✓	✓	✓	✓

Service Route Configuration Settings	Global		Virtual System	
	IPv4	IPv6	IPv4	IPv6
MDM—Mobile Device Management server.	✓	✓	–	–
Multi-Factor Authentication—Multi-factor authentication (MFA) server.	✓	✓	✓	✓
NetFlow—NetFlow collector for collecting network traffic statistics.	✓	✓	✓	✓
NTP—Network Time Protocol server.	✓	✓	–	–
Palo Alto Networks Services—Updates from Palo Alto Networks® and the public WildFire® server. This is also the service route for forwarding pre-10.0 telemetry data to Palo Alto Networks. (Current telemetry support forwards its data to Cortex Data Lake. This service route is not used in that case.)	✓	–	–	–
Panorama—Panorama management server.	✓	✓	–	–
Panorama Log Forwarding (PA-5200 Series firewalls only)—Log forwarding from the firewall to Log Collectors.	✓	✓	–	–
Proxy—Server that is acting as Proxy to the firewall.	✓	✓	–	–
RADIUS—Remote Authentication Dial-in User Service server.	✓	✓	✓	✓
SCEP—Simple Certificate Enrollment Protocol for requesting and distributing client certificates.	✓	✓	✓	–
SNMP Trap—Simple Network Management Protocol trap server.	✓	–	✓	–
Syslog—Server for system message logging.	✓	✓	✓	✓
TACACS+—Terminal Access Controller Access-Control System Plus (TACACS+) server for authentication, authorization, and accounting (AAA) services.	✓	✓	✓	✓
UID Agent—User-ID Agent server.	✓	✓	–	✓
URL Updates—Uniform Resource Locator (URL) updates server.	✓	✓	–	–

Service Route Configuration Settings	Global		Virtual System	
	IPv4	IPv6	IPv4	IPv6
VM Monitor—Monitoring Virtual Machine information, when you have enabled Device > VM Information Sources. *VM-Series firewalls in public cloud deployments that are monitoring virtual machines, must use the MGT interface. You cannot use a dataplane interface as a service route.*	✓	✓	✓	✓
WildFire Private—Private Palo Alto Networks WildFire server.	✓	–	–	–

When customizing a **Global** service route, select **Service Route Configuration** and, on the **IPv4** or **IPv6** tab, select a service from the list of available services; you can also select multiple services and **Set Selected Service Routes** to configure multiple service routes at once. To limit the selections in the **Source Address** drop-down, select a **Source Interface** and then a **Source Address** (from that interface). A Source Interface that is set to **Any** allows you to select a Source Address from any of the available interfaces. The Source Address displays the IPv4 or IPv6 address assigned to the selected interface and the selected IP address will be the source for the service traffic. You can **Use default** if you want the firewall to use the management interface for the service route; however, if the packet destination IP address matches the configured Destination IP address, the source IP address will be set to the Source Address configured for the Destination. You do not have to define a destination address because the destination is configured when you configure each service. For example, when you define your DNS servers (**Device** > **Setup** > **Services**), you will set the destination for DNS queries. You can specify both an IPv4 and an IPv6 address for a service.

An alternative way to customize a **Global** service route is to select **Service Route Configuration** and select **Destination**. Specify a **Destination** IP address to which an incoming packet is compared. If the packet destination address matches the configured Destination IP address, the source IP address is set to the Source Address configured for the Destination. To limit the selections in the **Source Address** drop-down, select a **Source Interface** and then select a **Source Address** (from that interface). A Source Interface that is set to **Any** allows you to select a Source Address from any of the interfaces available. The **MGT** Source Interface causes the firewall to use the management interface for the service route.

When you configure service routes for a **Virtual System**, choosing to **Inherit Global Service Route Configuration** means that all services for the virtual system will inherit the global service route settings. You can, instead, choose **Customize**, select **IPv4** or **IPv6**, and select a service; you can also select multiple services and **Set Selected Service Routes**. The **Source Interface** has the following three choices:

- **Inherit Global Setting**—The selected services inherit the global settings for those services.
- **Any**—Allows you to select a Source Address from any of the interfaces available (interfaces in the specific virtual system).
- **An interface from the drop-down**—Limits the drop-down for **Source Address** to the IP addresses for this interface.

For **Source Address**, select an address from the drop-down. For the services selected, server responses are sent to this source address.

Destination Service Route

- Device > Setup > Services > Global

On the **Global** tab, when you click on **Service Route Configuration** and then **Customize**, the **Destination** tab appears. Destination service routes are available under the **Global** tab only (not the **Virtual Systems** tab), so that the service route for an individual virtual system cannot override route table entries that are not associated with that virtual system.

You can use a destination service route to add a customized redirection of a service that is not supported on the **Customize** list of services. A destination service route is a way to set up routing to override the forwarding information base (FIB) route table. Any settings in the Destination service routes override the route table entries. They could be related or unrelated to any service.

The **Destination** tab is for the following use cases:

- When a service does not have an application service route.
- Within a single virtual system, when you want to use multiple virtual routers or a combination of virtual router and management port.

Destination Service Route Settings	Description
Destination	Enter the **Destination** IP address. An incoming packet with a destination address that matches this address will use as its source the Source Address you specify for this service route.
Source Interface	To limit the drop-down for Source Address, select a **Source Interface**. Selecting **Any** causes all IP addresses on all interfaces to be available in the Source Address drop-down. Selecting **MGT** causes the firewall to use the MGT interface for the service route.
Source Address	Select the **Source Address** for the service route; this address will used for packets returning from the destination. You do not need to enter the subnet for the destination address.

Device > Setup > Interfaces

Use this page to configure connection settings, allowed services, and administrative access for the management (MGT) interface on all firewall models and for the auxiliary interfaces (AUX-1 and AUX-2) on PA-5200 Series firewalls.

Palo Alto Networks recommends that you always specify the IP address and netmask (for IPv4) or prefix length (for IPv6) and the default gateway for every interface. If you omit any of these settings for the MGT interface (such as the default gateway), you can access the firewall only through the console port for future configuration changes.

To configure the MGT interface on the M-500 appliance or the Panorama virtual appliance, see Panorama > Setup > Interfaces*.*

*You can use a loopback interface as an alternative to the MGT interface for firewall management (*Network > Interfaces > Loopback*).*

Item	Description
Type (MGT interface only)	Select one: • **Static**—Requires you to enter the **IP Address** (IPv4), **Netmask** (IPv4), and **Default Gateway** manually. • **DHCP Client**—Configures the MGT interface as a DHCP client so that the firewall can send DHCP Discover or Request messages to find a DHCP server. The server responds by providing an IP address (IPv4), netmask (IPv4), and default gateway for the MGT interface. DHCP on the MGT interface is turned off by default for the VM-Series firewall (except for the VM-Series firewall in AWS and Azure).If you select **DHCP Client**, optionally select either or both of the following Client Options: • **Send Hostname**—Causes the MGT interface to send its hostname to the DHCP server as part of DHCP Option 12. • **Send Client ID**—Causes the MGT interface to send its client identifier as part of DHCP Option 61. If you select **DHCP Client**, optionally click **Show DHCP Client Runtime Info** to view the dynamic IP interface status: • Interface—Indicates MGT interface. • IP Address—IP address of the MGT interface. • Netmask—Subnet mask for the IP address, which indicates which bits are network or subnetwork and which bits are host. • Gateway—Default gateway for traffic leaving the MGT interface. • Primary/Secondary NTP—IP address of up to two NTP servers serving the MGT interface. If the DHCP Server returns NTP server addresses, the firewall considers them only if you did not manually configure NTP server addresses. If you manually configured NTP server addresses, the firewall does not overwrite them with those from the DHCP server. • Lease Time—Number of days, hours, minutes, and seconds that the DHCP IP address is assigned. • Expiry Time—Year/Month/Day, Hours/Minutes/Seconds, and time zone, indicating when DHCP lease will expire.

Item	Description
	• DHCP Server—IP address of the DHCP Server responding to MGT interface DHCP Client. • Domain—Name of domain to which the MGT interface belongs. • DNS Server—IP address of up to two DNS servers serving the MGT interface. If the DHCP Server returns DNS server addresses, the firewall considers them only if you did not manually configure DNS server addresses. If you manually configured DNS server addresses, the firewall does not overwrite them with those from the DHCP server. Optionally, you can **Renew** the DHCP lease for the IP address assigned to the MGT interface. Otherwise, **Close** the window.
Aux 1 / Aux 2 (PA-5200 Series firewalls only)	Select any of the following options to enable an auxiliary interface. These interfaces provide 10Gbps (SFP+) throughput for: • Firewall management traffic—You must enable the Network Services (protocols) that administrators will use when accessing the web interface and CLI to manage the firewall.  *Enable HTTPS instead of HTTP for the web interface and enable SSH instead of Telnet for the CLI.* • High availability (HA) synchronization between firewall peers—After configuring the interface, you must select it as the HA Control Link (**Device** > **High Availability** > **General**). • Log forwarding to Panorama—You must configure a service route with the **Panorama Log Forwarding** service enabled (Device > Setup > Services).
IP Address (IPv4)	If your network uses IPv4, assign an IPv4 address to the interface. Alternatively, you can assign the IP address of a loopback interface for firewall management (see Network > Interfaces > Loopback). By default, the IP address you enter is the source address for log forwarding.
Netmask (IPv4)	If you assigned an IPv4 address to the interface, you must also enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to the interface, you must also assign an IPv4 address to the default gateway (the gateway must be on the same subnet as the interface).
IPv6 Address/Prefix Length	If your network uses IPv6, assign an IPv6 address to the interface. To indicate the netmask, enter an IPv6 prefix length (for example, 2001:400:f00::1/64).
Default IPv6 Gateway	If you assigned an IPv6 address to the interface, you must also assign an IPv6 address to the default gateway (the gateway must be on the same subnet as the interface).
Speed	Configure a data rate and duplex option for the interface. The choices include 10Mbps, 100Mbps, and 1Gbps at full or half duplex. Use the default auto-negotiate setting to have the firewall determine the interface speed.

Item	Description
	This setting must match the port settings on the neighboring network equipment. To ensure matching settings, select auto-negotiate if the neighboring equipment supports that option.
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576 to 1,500; default is 1,500).
Administrative Management Services	• **HTTP**—Use this service to access the firewall web interface. *HTTP uses plaintext, which is not as secure as HTTPS. Therefore, Palo Alto Networks recommend you enable HTTPS instead of HTTP for management traffic on the interface.* • **Telnet**—Use this service to access the firewall CLI. *Telnet uses plaintext, which is not as secure as SSH. Therefore, Palo Alto Networks recommend you enable SSH instead of Telnet for management traffic on the interface.* • **HTTPS**—Use this service for secure access to the firewall web interface. • **SSH**—Use this service for secure access to the firewall CLI.
Network Services	Select the services you want to enable on the interface: • **HTTP OCSP**—Use this service to configure the firewall as an Online Certificate Status Protocol (OCSP) responder. For details, see Device > Certificate Management > OCSP Responder. • **Ping**—Use this service to test connectivity with external services. For example, you can ping the interface to verify it can receive PAN-OS software and content updates from the Palo Alto Networks Update Server. In a high availability (HA) deployment, HA peers use ping to exchange heartbeat backup information. • **SNMP**—Use this service to process firewall statistics queries from an SNMP manager. For details, see Enable SNMP Monitoring. • **User-ID**—Use this service to enable Redistribution of user mappings among firewalls. • **User-ID Syslog Listener-SSL**—Use this service to enable the PAN-OS integrated User-ID™ agent to collect syslog messages over SSL. For details, see Configure Access to Monitored Servers. • **User-ID Syslog Listener-UDP**—Use this service to enable the PAN-OS integrated User-ID agent to collect syslog messages over UDP. For details, see Configure Access to Monitored Servers.
Permitted IP Addresses	Enter the IP addresses from which administrators can access the firewall through the interface. An empty list (default) specifies that access is available from any IP address. *Do not leave the list blank; specify only the IP addresses of firewall administrators to prevent unauthorized access.*

Device > Setup > Telemetry

Telemetry is the process of collecting and transmitting data for threat and support analysis, and to enable application logic. To collect and transmit telemetry to Palo Alto Networks, you must first select a destination region. If your organization currently has a Cortex Data Lake license, then your destination region is limited to the region where your Cortex Data Lake instance resides.

Telemetry data is used to power applications that increase your ability to manage and configure your Palo Alto Networks products and services. These apps offer you improved visibility into device health, performance, capacity planning, and configuration. Palo Alto Networks also continually uses this data to improve threat prevention, and to help you maximize your product usage benefits.

Select **Device** > **Setup** > **Telemetry** to see the currently collected telemetry categories. To change these categories, edit the Telemetry widget. Deselect any categories that you don't want the firewall to collect, and commit your change.

Generate Telemetry File to obtain a live example of the data that the firewall will send to Palo Alto Networks at the next telemetry transmission interval.

To disable telemetry transmission entirely, make sure **Enable Telemetry** is not checked, and commit your change.

Device > Setup > Content-ID

Use the **Content-ID™** tab to define settings for URL filtering, data protection, and container pages.

Content-ID Settings	Description
URL Filtering	
Dynamic URL Cache Timeout	Click **Edit** and enter the timeout in hours. This value is used in dynamic URL filtering to determine the length of time an entry remains in the cache after it is returned from the URL filtering service. This option is applicable to URL filtering using the BrightCloud database only. For more on URL filtering, select Objects > Security Profiles > URL Filtering.
URL Continue Timeout	Specify the interval following a user's **Continue** action before the user must press continue again for URLs in the same category (range is 1 to 86,400 minutes; default is 15).
URL Admin Override Timeout	Specify the interval after the user enters the **Admin Override** password before the user must re-enter that password for URLs in the same category (range is 1 to 86,400 minutes; default is 15).
Hold Client Request for Category Lookup	Enable this option to specify that when the firewall cannot find category information for a URL in its local cache, it holds the web request as it queries PAN-DB.  *This option is disabled by default. Enable it as part of a best practice URL Filtering profile.*
Category Lookup Timeout (sec)	Specify the amount of time, in seconds, that the firewall will try to look up the category for a URL before determining that the category is `not-resolved` (range is 1 to 60 seconds; default is 2).
URL Admin Lockout Timeout	Specify the period of time that a user is locked out from attempting to use the URL Admin Override password after three unsuccessful attempts (range is 1 to 86,400 minutes; default is 30).
PAN-DB Server (Required for connecting to a private PAN-DB server)	Specify the IPv4 address, IPv6 address, or FQDN for the private PAN-DB servers on your network. You can add up to 20 entries. The firewall connects to the public PAN-DB cloud by default. The private PAN-DB solution is for enterprises that do not allow firewalls to directly access the PAN-DB servers in the public cloud. The firewalls access the servers included in this PAN-DB server list for the URL database, URL updates, and URL lookups for categorizing web pages.
URL Admin Override	
Settings for URL Admin Override	For each virtual system that you want to configure for URL admin override, **Add** and specify the settings that apply when a URL filtering profile blocks a

Content-ID Settings	Description
	page and the **Override** action is specified For details, see Objects > Security Profiles > URL Fiiltering. • **Location**—(multi-vsys firewalls only) Select the virtual system from the drop-down. • **Password/Confirm Password**—Enter the password that the user must enter to override the block page. • **SSL/TLS Service Profile**—To specify a certificate and the allowed TLS protocol versions for securing communications when redirecting through the specified server, select an SSL/TLS Service profile. For details, see Device > Certificate Management > SSL/TLS Service Profile. • **Mode**—Determines whether the block page is delivered transparently (it appears to originate at the blocked website) or redirects the user to the specified server. If you choose **Redirect**, then enter the IP address for redirection. You can also **Delete** an entry.
Content Cloud Settings	
Service URL	The Cloud Services server URL to scan Enterprise Data Loss Prevention (DLP) files. • **APAC**—**`apac.hawkeye.services-edge.paloaltonetworks.com`** • **Europe**—**`eu.hawkeye.services-edge.paloaltonetworks.com`** • **United States**—**`us.hawkeye.services-edge.paloaltonetworks.com`**
Content-ID Settings	
Allow Forwarding of Decrypted Content	Enable this option to configure the firewall to forward decrypted content to an outside service when port mirroring or sending WildFire® files for analysis.  *Enable this option and send all unknown files in decrypted traffic to WildFire for analysis.* For a firewall with multiple virtual system (multi-vsys) capability, you enable this option individually for each virtual system. Select **Device** > **Virtual Systems** and select the virtual system on which you want to enable forwarding of decrypted content. This option is available in the Virtual System dialog.
Extended Packet Capture Length	Set the number of packets to capture when the extended-capture option is enabled in Anti-Spyware and Vulnerability Protection profiles (range is 1 to 50; default is 5).
Forward Segments Exceeding TCP App-ID™ Inspection Queue	Enable this option to forward segments and classify the application as `unknown-tcp` when the App-ID queue exceeds the 64-segment limit. Use the following global counter to view the number of segments in excess of this queue regardless of whether you enabled or disabled this option:

Content-ID Settings	Description
	`appid_exceed_queue_limit` Disable this option to prevent the firewall from forwarding TCP segments and skipping App-ID inspection when the App-ID inspection queue is full.  *This option is disabled by default and you should leave it disabled for maximum security.*  *When you disable this option, you may notice increased latency on streams where more than 64 segments were queued awaiting App-ID processing.*

Forward Segments Exceeding TCP Content Inspection Queue	Enable this option to forward TCP segments and skip content inspection when the TCP content inspection queue is full. The firewall can queue up to 64 segments while waiting for the content engine. When the firewall forwards a segment and skips content inspection due to a full content inspection queue, it increments the following global counter:
	
	`ctd_exceed_queue_limit`
	
	Disable this option to prevent the firewall from forwarding TCP segments and skipping content inspection when the content inspection queue is full. When you disable this option, the firewall drops any segments that exceed the queue limit and increments the following global counter:
	
	`ctd_exceed_queue_limit_drop`
	
	This pair of global counters applies to both TCP and UDP packets. If, after viewing the global counters, you decide to change the setting, you can modify it from within the CLI using the following CLI command:
	
	`set deviceconfig setting ctd tcp-bypass-exceed-queue`
	
	  *This option is enabled by default but Palo Alto Networks recommends that you disable this option for maximum security. However, due to TCP retransmissions for dropped traffic, disabling this option can result in performance degradation and some applications can incur loss of functionality—particularly in high-volume traffic environments.*

Forward Datagrams Exceeding UDP Content Inspection Queue	Enable this option to forward UDP datagrams and skip content inspection when the UDP content inspection queue is full. The firewall can queue up to 64 datagrams while waiting for a response from the content engine. When the firewall forwards a datagram and skips content inspection due to a UDP content inspection queue overflow, it increments the following global counter:

Content-ID Settings	Description

	`ctd_exceed_queue_limit`
	
	Disable this option to prevent the firewall from forwarding datagrams and skipping content inspection when the UDP content inspection queue is full. With this option disabled, the firewall drops any datagrams that exceed the queue limit and increments the following global counter:
	
	`ctd_exceed_queue_limit_drop`
	
	This pair of global counters applies to both TCP and UDP packets. If, after viewing the global counters, you decide to change the setting, you can modify it from within the CLI using the following command:
	
	`set deviceconfig setting ctd udp-bypass-exceed-queue`
	
	  *This option is enabled by default but Palo Alto Networks recommends that you disable this option for maximum security. However, due to dropped packets, disabling this option can result in performance degradation and some applications can incur loss of functionality—particularly in high-volume traffic environments.*

Allow HTTP partial response	Enable this HTTP partial response option to enable a client to fetch only part of a file. When a next-generation firewall in the path of a transfer identifies and drops a malicious file, it terminates the TCP session with an RST packet. If the web browser implements the HTTP Range option, it can start a new session to fetch only the remaining part of the file. This prevents the firewall from triggering the same signature again due to the lack of context into the initial session while, at the same time, allows the web browser to reassemble the file and deliver the malicious content; to prevent this, make sure to disable this option.  *By default, Allow HTTP partial response is enabled but Palo Alto Networks recommends that you disable this option for maximum security. Disabling this option should not impact device performance; however, HTTP file transfer interruption recovery may be impaired. In addition, disabling this option can impact streaming media services, such as Netflix, Microsoft Updates, and Palo Alto Networks content updates.*
Real-Time Signature Lookup	
DNS Signature Lookup Timeout (ms)	Specify the duration of time, in milliseconds, for the firewall to query the DNS Security service. If the cloud does not respond before the end of the specified period, the firewall releases the associated DNS response to the requesting client (range is 0 to 60,000; default is 100).

Content-ID Settings	Description
X-Forwarded-For Headers	
Use X-Forwarded-For Header	*You cannot enable X-Forwarded-For for User-ID and Security Policy at the same time.* • **Disabled**—When disabled, the firewall does not read the IP addresses from X-Forwarded-For (XFF) header in client requests. • **Enable for User-ID**—Enable this option to specify that User-ID reads IP addresses from the X-Forwarded-For (XFF) header in client requests for web services when the firewall is deployed between the internet and a proxy server that would otherwise hide client IP addresses. User-ID matches the IP addresses it reads with usernames that your policies reference so that those policies can control and log access for the associated users and groups. If the header has multiple IP addresses, User-ID uses the first entry from the left. In some cases, the header value is a character string instead of an IP address. If the string matches a username that User-ID mapped to an IP address, the firewall uses that username for group mapping references in policies. If no IP address-mapping exists for the string, the firewall invokes the policy rules in which the source user is set to **any** or **unknown**. URL Filtering logs display the matched usernames in the Source User field. If User-ID cannot perform the matching or is not enabled for the zone associated with the IP address, the Source User field displays the XFF IP address with the prefix **`x-fwd-for`**. *Enable using the XFF header in User-ID so that the original client IP address appears in the logs to help you when you need to investigate an issue.* • **Enable for Security Policy**—Enable this option to specify that the firewall reads the IP addresses from the X-Forwarded-For (XFF) header in client requests for web services when an upstream device, such as proxy server or load balancer, is deployed between the client and the firewall. The proxy server or load balancer IP address replaces the client IP address as the request source IP. The firewall can then uses the IP addresses in the XFF header to enforce policy. *The firewall uses the IP address most-recently added to the XFF field. If the request passes through multiple upstream devices, the firewall applies policy based on which ever IP address was added last.*
Strip-X-Forwarded-For Header	Enable this option to remove the X-Forwarded-For (XFF) header, which contains the IP address of a client requesting a web service when the firewall is deployed between the internet and a proxy server. The firewall zeroes out the header value before forwarding the request: the forwarded packets don't contain internal source IP information.

Content-ID Settings	Description
	Enabling this option does not disable the use of XFF headers for user attribution in policies; the firewall zeroes out the XFF value only after using it for user attribution. *When you enable the use of XFF headers in User-ID, also enable stripping the XFF header before forwarding the packet to protect user privacy without losing the ability to track users. Enabling both options allows you to log and track original user IP addresses while at the same time protecting user privacy by not forwarding their original IP address.*
Content-ID Features	
Manage Data Protection	Add additional protection for access to logs that may contain sensitive information, such as credit card or social security numbers. Click **Manage Data Protection** to perform the following tasks: • **Set Password**—If one is not already configured, enter and confirm a new password. • **Change Password**—Enter the old password and enter and confirm the new password. • **Delete Password**—Deletes the password and the data that was protected.
Container Pages	Use these settings to specify the types of URLs that the firewall will track or log based on content type, such as application/pdf, application/soap+xml, application/xhtml+, text/html, text/plain, and text/xml. Container pages are set per virtual system, which you select from the **Location** drop-down. If a virtual system does not have an explicit container page defined, the firewall uses the default content types. **Add** and enter a content type or select an existing content type. Adding new content types for a virtual system overrides the default list of content types. If there are no content types associated with a virtual system, the default list of content types is used.

Device > Setup > WildFire

Select **Device** > **Setup** > **WildFire** to configure WildFire settings on the firewall and Panorama. You can enable both the WildFire cloud and a WildFire appliance to be used to perform file analysis. You can also set file size limits and session information that will be reported. After populating WildFire settings, you can specify what files to forward to the WildFire cloud or the WildFire appliance by creating a **WildFire Analysis** profile (**Objects** > **Security Profiles** > **WildFire Analysis**).

To forward decrypted content to WildFire, refer to Forward Decrypted SSL Traffic for WildFire Analysis.

WildFire Settings	Description
General Settings	
WildFire Public Cloud	Enter **`wildfire.paloaltonetworks.com`** to send files to the WildFire global cloud, hosted in the United States, for analysis. Alternatively, you can instead send files to a WildFire regional cloud for analysis. Regional clouds are designed to adhere to the data privacy expectations you might have depending on your location. *Forward samples to a regional WildFire cloud to ensure adherence to the data privacy and compliance standards specific to your region. Regional clouds are:* • *Europe—**`eu.wildfire.paloaltonetworks.com`*** • *Japan—**`jp.wildfire.paloaltonetworks.com`*** • *Singapore—**`sg.wildfire.paloaltonetworks.com`***
WildFire Private Cloud	Specify the IPv4/IPv6 address or FQDN of the WildFire appliance. The firewall sends files for analysis to the specified WildFire appliance. Panorama collects threat IDs from the WildFire appliance to enable the addition of threat exceptions in Anti-Spyware profiles (for DNS signatures only) and Antivirus profiles that you configure in device groups. Panorama also collects information from the WildFire appliance to populate fields that are missing in the WildFire Submissions logs received from firewalls running software versions earlier than PAN-OS 7.0.
File Size Limits	Specify the maximum file size that will be forwarded to the WildFire server. For all best practice recommendations about file size limits, if the limit is too large and prevents the firewall from forwarding multiple large zero-day files at the same time, lower and tune the maximum limit based on the amount of available firewall buffer space. If more buffer space is available, you can increase the file size limit above the best practice recommendation. The best practice recommendations are a good starting place for setting effective limits that don't overtax firewall resources. Available ranges are: • **pe** (Portable Executable)—Range is 1 to 50MB; default is 16MB. *Set the size for PE files to 16MB.*

WildFire Settings	Description
	• **apk** (Android Application)—Range is 1 to 50MB; default 10MB.  *Set the size for APK files to 10MB.* • **pdf** (Portable Document Format)—Range is 100KB to 51,200KB; default is 3,072KB.  *Set the size for PDF files to 3,072KB.* • **ms-office** (Microsoft Office)—Range is 200KB to 51,200KB; default is 16,384KB.  *Set the size for ms-office files to 16,384KB.* • **jar** (Packaged Java class file)—Range is 1 to 20MB; default is 5MB.  *Set the size for jar files to 5MB.* • **flash** (Adobe Flash)—Range is 1 to 10MB; default is 5MB.  *Set the size for flash files to 5MB.* • **MacOSX** (DMG/MAC-APP/MACH-O PKG files)—Range is 1 to 50MB; default is 10MB.  *Set the size for MacOSX files to 1MB.* • **archive** (RAR and 7z files)—Range is 1 to 50MB; default is 50MB.  *Set the size for archive files to 50MB.* • **linux** (ELF files)—Range is 1 to 50MB; default is 50MB.  *Set the size for linux files to 50MB.* • **script** (JScript, VBScript, PowerShell, and Shell Script files)—Range is 10 to 4096KB; default is 20KB.  *Set the size for script files to 20KB.*  *The preceding values might differ based on the current version of PAN-OS or the content release. To see valid ranges, click in the Size Limit field; a pop-up displays the available range and default value.*

WildFire Settings	Description
Report Benign Files	When this option is enabled (disabled by default), files analyzed by WildFire that are determined to be benign will appear in the **Monitor** > **WildFire Submissions** log. Even if this option is enabled on the firewall, email links that WildFire deems benign will not be logged because of the potential quantity of links processed.
Report Grayware Files	When this option is enabled (disabled by default), files analyzed by WildFire that are determined to be grayware will appear in the **Monitor** > **WildFire Submissions** log.  *Even if this option is enabled on the firewall, email links that WildFire determines to be grayware will not be logged because of the potential quantity of links processed.*  *Enable reporting grayware files to log session information, network activity, host activity, and other information that helps with analytics.*
Session Information Settings	
Settings	Specify the information to be forwarded to the WildFire server. By default, all are selected and the best practice is to forward all session information to provide statistics and other metrics that enable you to take actions to prevent threat events: • **Source IP**—Source IP address that sent the suspected file. • **Source Port**—Source port that sent the suspected file. • **Destination IP**—Destination IP address for the suspected file. • **Destination Port**—Destination port for the suspected file. • **Vsys**—Firewall virtual system that identified the possible malware. • **Application**—User application that was used to transmit the file. • **User**—Targeted user. • **URL**—URL associated with the suspected file. • **Filename**—Name of the file that was sent. • **Email sender**—Provides the sender name in WildFire logs and WildFire detailed reports when a malicious email link is detected in SMTP and POP3 traffic. • **Email recipient**—Provides the recipient name in WildFire logs and WildFire detailed reports when a malicious email link is detected in SMTP and POP3 traffic. • **Email subject**—Provides the email subject in WildFire logs and WildFire detailed reports when a malicious email link is detected in SMTP and POP3 traffic.

Device > Setup > Session

Select **Device** > **Setup** > **Session** to configure session age-out times, decryption certificate settings, and global session-related settings such as firewalling IPv6 traffic and rematching Security policy to existing sessions when the policy changes. The tab has the following sections:

- Session Settings
- Session Timeouts
- TCP Settings
- Decryption Settings: Certificate Revocation Checking
- Decryption Settings: Forward Proxy Server Certificate Settings
- VPN Session Settings

Session Settings

The following table describes session settings.

Session Settings	Description
Rematch Sessions	Click **Edit** and select **Rematch Sessions** to cause the firewall to apply newly configured security policy rules to sessions that are already in progress. This capability is enabled by default. If this setting is disabled, any policy rule change applies to only those sessions initiated after the change was committed. For example, if a Telnet session started while an associated policy rule was configured that allowed Telnet, and you subsequently committed a policy rule change to deny Telnet, the firewall applies the revised policy rule to the current session and blocks it.  *Enable Rematch Sessions to apply your latest Security policy rules to currently active sessions.*
ICMPv6 Token Bucket Size	Enter the bucket size for rate limiting of ICMPv6 error messages. The token bucket size is a parameter of the token bucket algorithm that controls how bursty the ICMPv6 error packets can be (range is 10 to 65,535 packets; default is 100).
ICMPv6 Error Packet Rate	Enter the average number of ICMPv6 error packets per second allowed globally through the firewall (range is 10 to 65,535; default is 100). This value applies to all interfaces. If the firewall reaches the ICMPv6 error packet rate, the ICMPv6 token bucket is used to enable throttling of ICMPv6 error messages.
Enable IPv6 Firewalling	To enable firewall capabilities for IPv6 traffic, **Edit** and select **IPv6 Firewalling**. The firewall ignores all IPv6-based configurations if you do not enable IPv6 firewalling. Even if you enable IPv6 traffic on an interface, you must also enable the **IPv6 Firewalling** option for IPv6 firewalling to function.

Session Settings	Description
Enable Jumbo Frame Global MTU	Select to enable jumbo frame support on Ethernet interfaces. Jumbo frames have a maximum transmission unit (MTU) of 9,192 bytes and are available only on certain models. • If you do not **Enable Jumbo Frame**, the **Global MTU** defaults to 1,500 bytes (range is 576 to 1,500). • If you **Enable Jumbo Frame**, the **Global MTU** defaults to 9,192 bytes (range is 9,192 to 9,216 bytes).  *Jumbo frames can take up to five times more memory compared to normal packets and can reduce the number of available packet buffers by 20%. This reduces the queue sizes dedicated for out-of-order, application identification, and other such packet processing tasks. Beginning with PAN-OS 8.1, if you enable the jumbo frame global MTU configuration and reboot your firewall, packet buffers are redistributed to process jumbo frames more efficiently.* If you enable jumbo frames and you have interfaces where the MTU is not specifically configured, those interfaces automatically inherit the jumbo frame size. Therefore, before you enable jumbo frames, if you have any interface on which you do not want to allow jumbo frames, you must set the MTU for that interface to 1,500 bytes or another value. To configure the MTU for the interface (**Network** > **Interfaces** > **Ethernet**), see PA-7000 Series Layer 3 Interface.
DHCP Broadcast Session	If your firewall is acting as a DHCP server, select this option to enable session logs for DHCP broadcast packets. The DHCP Broadcast Session option enables generation of Enhanced Application Logs (EAL logs) for DHCP for use by IoT Security and other services. If you do not enable this option, the firewall forwards the packets without creating logs for the DHCP broadcast packets.
NAT64 IPv6 Minimum Network MTU	Enter the global MTU for IPv6 translated traffic. The default of 1,280 bytes is based on the standard minimum MTU for IPv6 traffic (range is 1,280 to 9,216).
NAT Oversubscription Rate	Select the DIPP NAT oversubscription rate, which is the number of times that the firewall can use the same translated IP address and port pair concurrently. Reducing the oversubscription rate decreases the number of source device translations but will provide higher NAT rule capacities. • **Platform Default**—Explicit configuration of the oversubscription rate is turned off and the default oversubscription rate for the model applies. (See default rates of firewall models at https://www.paloaltonetworks.com/products/product-selection.html). • **1x**—1 time. This means no oversubscription; the firewall cannot use the same translated IP address and port pair more than once concurrently. • **2x**—2 times • **4x**—4 times • **8x**—8 times

Session Settings	Description
ICMP Unreachable Packet Rate (per sec)	Define the maximum number of ICMP Unreachable responses that the firewall can send per second. This limit is shared by IPv4 and IPv6 packets. Default value is 200 messages per second (range is 1 to 65,535).
Accelerated Aging	Enables accelerated age-out of idle sessions. Select this option to enable accelerated aging and specify the threshold (%) and scaling factor. When the session table reaches the **Accelerated Aging Threshold** (% full), PAN-OS applies the **Accelerated Aging Scaling Factor** to the aging calculations for all sessions. The default scaling factor is 2, meaning that accelerated aging occurs at a rate twice as fast as the configured idle time. The configured idle time divided by 2 results in a faster timeout (one-half the time). To calculate the accelerated aging of a session, PAN-OS divides the configured idle time (for that type of session) by the scaling factor to determine a shorter timeout. For example, if the scaling factor is 10, a session that would normally time out after 3,600 seconds will time out 10 times faster (in 1/10 of the time), which is 360 seconds.  *Enable an accelerated aging threshold and set an acceptable scaling factor to free up session table space faster when the session table begins to fill up.*
Packet Buffer Protection	Beginning in PAN-OS 10.0, Packet Buffer Protection is enabled by default globally and on each zone. As a best practice, keep packet buffer protection enabled globally and on each zone to protect the firewall buffers from DoS attacks and aggressive sessions and sources. This option protects the receive buffers on the firewall from attacks or abusive traffic that causes system resources to back up and legitimate traffic to get dropped. Packet buffer protection identifies offending sessions, uses Random Early Detection (RED) as a first line of defense, and discards the session or blocks the offending IP address if abuse continues. If the firewall detects many small sessions or rapid session creation (or both) from a particular IP address, it blocks that IP address. Take baseline measurements of firewall packet buffer utilization to understand the firewall capacity and ensure that the firewall is properly configured so that only an attack causes a large spike in buffer usage. • **Alert (%)**—When packet buffer utilization exceeds this threshold for more than 10 seconds, the firewall creates a log event every minute. The firewall generates log events when packet buffer protection is enabled globally (range is 0% to 99%; default is 50%). If the value is 0%, the firewall does not create a log event. Start with the default threshold value and adjust as necessary. • **Activate (%)**—When this threshold is reached, the firewall begins to mitigate the most abusive sessions (range is 0% to 99%; default is 80%). If the value is 0%, the firewall does not apply RED. Start with the default threshold value and adjust as necessary.

Session Settings	Description
Packet Buffer Protection (cont)	• (Hardware firewalls running PAN-OS 10.0 or a later release) As an alternative to packet buffer protection that is based on utilization percentages (described above), you can instead trigger packet buffer protection based on CPU processing latency by enabling **Buffering Latency Based** and configuring the following settings: • **Latency Alert (milliseconds)**—When latency exceeds this threshold, the firewall starts generating an Alert log event every minute (range is 1 to 20,000; default is 50). • **Latency Activate (milliseconds)**—When latency exceeds this threshold, the firewall activates Random Early Detection (RED) on incoming packets and starts generating an Activate log every 10 seconds (range is 1 to 20,000; default is 200). • **Latency Max Tolerate (milliseconds)**—When latency equals or exceeds this threshold, the firewall uses RED with close to 100% drop probability (range is 1 to 20,000ms; default is 500ms). If the current latency is a value between the Latency Activate threshold and the Latency Max Tolerate threshold, the firewall calculates the RED drop probability as follows: (current latency - **Latency Activate** threshold) / (**Latency Max Tolerate** threshold - (**Latency Activate** threshold). For example, if the current latency is 300, Latency Activate is 200, and Latency Max Tolerate is 500, then (300-200)/(500-200) = 1/3, meaning the firewall uses approximately 33% RED drop probability.
Packet Buffer Protection (cont)	• **Block Hold Time (sec)**—The amount of time, in seconds, that the session is allowed to continue before the session is discarded or the source IP address is blocked (range is 0 to 65,535; default is 60). This timer monitors RED-mitigated sessions to see if they are still pushing buffer utilization or latency above the configured threshold. If the abusive behavior continues past the block hold time, the session is discarded. If the value is 0, the firewall does not discard sessions based on packet buffer protection. Start with the default value, monitor packet buffer utilization or latency, and adjust the time value as necessary. • **Block Duration (sec)**—The amount of time, in seconds, that a discarded session remains discarded or a blocked IP address remains blocked (range is 1 to 15,999,999; default is 3,600). Use the default value unless blocking an IP address for one hour is too severe a penalty for your business conditions, in which case you can reduce the duration. Monitor packet buffer utilization or latency and adjust the duration as necessary.  *Network Address Translation (NAT) can increase packet buffer utilization. If this affects the buffer utilization, reduce the Block Hold Time to block individual sessions faster and reduce the Block Duration so other sessions from the underlying IP address aren't unduly penalized.*
Multicast Route Setup Buffering	Select this option (disabled by default) to enable multicast route setup buffering, which allows the firewall to preserve the first packet in a multicast session when the multicast route or forwarding information base (FIB) entry does not yet exist for the corresponding multicast group. By default, the

Session Settings	Description
	firewall does not buffer the first multicast packet in a new session; instead, it uses the first packet to set up the multicast route. This is expected behavior for multicast traffic. You only need to enable multicast route setup buffering if your content servers are directly connected to the firewall and your custom application cannot withstand the first packet in the session being dropped.
Multicast Route Setup Buffer Size	If you enable Multicast Route Setup Buffering, you can tune the buffer size, which specifies the buffer size per flow (range is 1 to 2,000; default is 1,000.) The firewall can buffer a maximum of 5,000 packets.

Session Timeouts

Some session timeouts define the duration for which PAN-OS maintains a session on the firewall after inactivity in the session. By default, when the session timeout for the protocol expires, PAN-OS closes the session. The Discard session timeouts define the maximum time that a session remains open after PAN-OS denies the session based on Security policy rules.

On the firewall, you can define a number of timeouts for TCP, UDP, ICMP, and SCTP sessions in particular. The **Default** timeout applies to any other type of session. All of these timeouts are global, meaning they apply to all of the sessions of that type on the firewall.

In addition to the global settings, you have the flexibility to define timeouts for an individual application in the **Objects** > **Applications** tab. The timeouts available for that application appear in the Options window. The firewall applies application timeouts to an application that is in Established state. When configured, timeouts for an application override the global TCP, UDP, or SCTP session timeouts.

Use the options in this section to configure global session timeout settings—specifically for TCP, UDP, ICMP, SCTP, and for all other types of sessions.

The defaults are optimal values and the best practice is to use the default values. However, you can modify these according to your network needs. Setting a value too low could cause sensitivity to minor network delays and could result in a failure to establish connections with the firewall. Setting a value too high could delay failure detection.

Session Timeouts Settings	Description
Default	Maximum length of time, in seconds, that a non-TCP/UDP, non-SCTP, or non-ICMP session can be open without a response (range is 1 to 15,999,999; default is 30).
Discard Default	Maximum length of time (in seconds) that a non-TCP/UDP/SCTP session remains open after PAN-OS denies the session based on Security policy rules configured on the firewall (range is 1 to 15,999,999; default is 60).
Discard TCP	Maximum length of time (in seconds) that a TCP session remains open after PAN-OS denies the session based on Security policy rules configured on the firewall (range is 1 to 15,999,999; default is 90).
Discard UDP	Maximum length of time (in seconds) that a UDP session remains open after PAN-OS denies the session based on Security policy rules configured on the firewall (range is 1 to 15,999,999; default is 60).

Session Timeouts Settings	Description
ICMP	Maximum length of time that an ICMP session can be open without an ICMP response (range is 1 to 15,999,999; default is 6).
Scan	Maximum length of time, in seconds, that a session can be inactive before the firewall clears the session and recovers the buffer resources the session was using. The inactive time is the length of time that has passed since the session was last refreshed by a packet or an event. Range is 5 to 30; default is 10.
TCP	Maximum length of time that a TCP session remains open without a response, after a TCP session is in the Established state (after the handshake is complete and/or data transmission has started); (range is 1 to 15,999,999; default is 3,600).
TCP handshake	Maximum length of time, in seconds, between receiving the SYN-ACK and the subsequent ACK to fully establish the session (ranges is 1 to 60; default is 10).
TCP init	Maximum length of time, in seconds, between receiving the SYN and SYN-ACK before starting the TCP handshake timer (ranges is 1 to 60; default is 5).
TCP Half Closed	Maximum length of time, in seconds, between receiving the first FIN and receiving the second FIN or a RST (range is 1 to 604,800; default is 120).
TCP Time Wait	Maximum length of time, in seconds, after receiving the second FIN or a RST (range is 1 to 600; default is 15).
Unverified RST	Maximum length of time, in seconds, after receiving a RST that cannot be verified (the RST is within the TCP window but has an unexpected sequence number, or the RST is from an asymmetric path); (ranges is 1 to 600; default is 30).
UDP	Maximum length of time, in seconds, that a UDP session remains open without a UDP response (range is 1 to 1,599,999; default is 30).
Authentication Portal	The authentication session timeout in seconds for the Authentication Portal web form (default is 30, range is 1 to 1,599,999). To access the requested content, the user must enter the authentication credentials in this form and be successfully authenticated. The authentication session timeout in seconds for the Authentication Portal web form (default is 30, range is 1 to 1,599,999). To access the requested content, the user must enter the authentication credentials in this form and be successfully authenticated.
SCTP INIT	Maximum length of time, in seconds, from receiving an SCTP INIT chunk that the firewall must receive the INIT ACK chunk before the firewall stops the SCTP association initiation (range is 1 to 60; default is 5).
SCTP COOKIE	Maximum length of time, in seconds, from receiving an SCTP INIT ACK chunk with the state COOKIE parameter that the firewall must receive the

Session Timeouts Settings	Description
	COOKIE ECHO chunk with the cookie before the firewall stops the SCTP association initiation (range is 1 to 600; default is 60).
Discard SCTP	Maximum length of time, in seconds, that an SCTP association remains open after PAN-OS denies the session based on Security policy rules configured on the firewall (range is 1 to 604,800; default is 30).
SCTP	Maximum length of time, in seconds, that can elapse without SCTP traffic for an association before all sessions in the association time out (range is 1 to 604,800; default is 3,600).
SCTP Shutdown	Maximum length of time, in seconds, that the firewall waits after an SCTP SHUTDOWN chunk to receive a SHUTDOWN ACK chunk before the firewall disregards the SHUTDOWN chunk (range is 1 to 600; default is 30).

TCP Settings

The following table describes TCP settings.

TCP Settings	Description
Forward segments exceeding TCP out-of-order queue	Select this option if you want the firewall to forward segments that exceed the TCP out-of-order queue limit of 64 per session. If you disable this option, the firewall drops segments that exceed the out-of-order queue limit. To see a count of the number of segments that the firewall dropped as a result of enabling this option, run the following CLI command: `show counter global tcp_exceed_flow_seg_limit` *This option is disabled by default and should remain this way for the most secure deployment. Disabling this option may result in increased latency for the specific stream that received over 64 segments out of order. There should be no loss of connectivity because the TCP stack should handle missing segments retransmission.*
Allow arbitrary ACK in response to SYN	Enable to globally reject the packet if the first packet for the TCP session setup is not a SYN packet. *To control the setting for individual Zone Protection Profiles, change the Reject Non-SYN TCP setting in TCP Drop.*
Drop segments with null timestamp option	The TCP timestamp records when the segment was sent and allows the firewall to verify that the timestamp is valid for that session, preventing TCP sequence number wrapping. The TCP timestamp is also used to calculate round trip time. With this option enabled, the firewall drops packets with

TCP Settings	Description
	null timestamps. To see a count of the number of segments that the firewall dropped as a result of enabling this option, run the following CLI command: `show counter global tcp_invalid_ts_option` *This option is enabled by default and should remain this way for the most secure deployment. Enabling this option should not result in performance degradation. However, if a network stack incorrectly generates segments with a null TCP timestamp option value, enabling this option may result in connectivity issues.*
Asymmetric Path	Set globally whether to drop or bypass packets that contain out-of-sync ACKs or out-of-window sequence numbers. • **Drop**—Drop packets that contain an asymmetric path. • **Bypass**—Bypass scanning on packets that contain an asymmetric path. *To control the setting for individual Zone Protection Profiles, change the Asymmetric Path setting in* TCP Drop.
Urgent Data Flag	Use this option to configure whether the firewall allows the urgent pointer (URG bit flag) in the TCP header. The urgent pointer in the TCP header is used to promote a packet for immediate processing—the firewall removes it from the processing queue and expedites it through the TCP/IP stack on the host. This process is called out-of-band processing. Because the implementation of the urgent pointer varies by host, setting this option to **Clear** (the default and recommended setting) eliminates any ambiguity by disallowing out-of-band processing so that the out-of-band byte in the payload becomes part of the payload and the packet is not processed urgently. Additionally, the **Clear** setting ensures that the firewall sees the exact stream in the protocol stack as the host for whom the packet is destined. To see a count of the number of segments in which the firewall cleared the URG flag when this option is set to **Clear**, run the following CLI command: `show counter global tcp_clear_urg` *By default, this flag is set to Clear and should remain this way for the most secure deployment. This should not result in performance degradation; in the rare instance that applications, such as telnet, are using the urgent data feature, TCP may be impacted. If you set this flag to Do Not Modify, the firewall allows packets with the URG bit flag in*

TCP Settings	Description
	the TCP header and enables out-of-band processing (not recommended).
Drop segments without flag	Illegal TCP segments without any flags set can be used to evade content inspection. With this option enabled (the default) the firewall drops packets that have no flags set in the TCP header. To see a count of the number of segments that the firewall dropped as a result of this option, run the following CLI command: `show counter global tcp_flag_zero` *This option is enabled by default and should remain this way for the most secure deployment. Enabling this option should not result in performance degradation. However, if a network stack incorrectly generates segments with no TCP flags, enabling this option may result in connectivity issues.*
Strip MPTCP option	Enabled globally by default to convert (Multipath TCP) MPTCP connections to standard TCP connections. *To allow MCTCP, change the Multipath TCP (MPTCP) Options setting in TCP Drop.*
SIP TCP cleartext	Select one of the following options to set the cleartext proxy behavior for SIP TCP sessions when a segmented SIP header is detected. • **Always Off**—Disables the cleartext proxy. Disable the proxy when the SIP message size is generally smaller than the MSS and when the SIP messages fit within a single segment, or if you need to ensure TCP proxy resources are reserved for SSL forward proxy or HTTP/2. • **Always enabled**—Default. Uses TCP proxy for all SIP over TCP sessions to help with the correct reassembly and ordering of TCP segments for proper ALG operation. • **Automatically enable proxy when needed**—When selected, the cleartext proxy is automatically enabled for sessions where the ALG detects SIP message fragmentation. Helps optimize the proxy when it is also used for SSL forward proxy or HTTP/2.
TCP Retransmit Scan (PAN-OS 10.0.2 or later)	If enabled, the checksum for the original packet is scanned when a retransmitted packet is seen. If the checksum are different between the original and retransmitted packet, the retransmitted packet is assumed to be malicious and dropped.

Decryption Settings: Certificate Revocation Checking

Select **Session**, and in Decryption Settings, select **Certificate Revocation Checking** to set the parameters described in the following table.

Session Features: Certificate Revocation Checking Settings	Description
Enable: CRL	Select this option to use the certificate revocation list (CRL) method to verify the revocation status of certificates. If you also enable Online Certificate Status Protocol (OCSP), the firewall first tries OCSP; if the OCSP server is unavailable, the firewall then tries the CRL method. For more information on decryption certificates, see Keys and Certificates for Decryption.
Receive Timeout: CRL	If you enabled the CRL method for verifying certificate revocation status, specify the interval in seconds (1 to 60; default is 5) after which the firewall stops waiting for a response from the CRL service.
Enable: OCSP	Select this option to use OCSP to verify the revocation status of certificates.
Receive Timeout: OCSP	If you enabled the OCSP method for verifying certificate revocation status, specify the interval in seconds (1 to 60; default is 5) after which the firewall stops waiting for a response from the OCSP responder.
Block Session With Unknown Certificate Status	Select this option to block SSL/TLS sessions when the OCSP or CRL service returns a certificate revocation status of unknown. Otherwise, the firewall proceeds with the session.
Block Session On Certificate Status Check Timeout	Select this option to block SSL/TLS sessions after the firewall registers a CRL or OCSP request timeout. Otherwise, the firewall proceeds with the session.
Certificate Status Timeout	Specify the interval in seconds (1 to 60; default is 5) after which the firewall stops waiting for a response from any certificate status service and applies any session blocking logic you optionally define. The **Certificate Status Timeout** relates to the OCSP/CRL **Receive Timeout** as follows: • If you enable both OCSP and CRL—The firewall registers a request timeout after the lesser of two intervals passes: the **Certificate Status Timeout** value or the aggregate of the two **Receive Timeout** values. • If you enable only OCSP—The firewall registers a request timeout after the lesser of two intervals passes: the **Certificate Status Timeout** value or the OCSP **Receive Timeout** value. • If you enable only CRL—The firewall registers a request timeout after the lesser of two intervals passes: the **Certificate Status Timeout** value or the CRL **Receive Timeout** value.

Decryption Settings: Forward Proxy Server Certificate Settings

In Decryption Settings (**Session** tab), select **SSL Forward Proxy Settings** to configure the **RSA Key Size** or **ECDSA Key Size** and the hashing algorithm for the certificates that the firewall presents to clients when establishing sessions for SSL/TLS Forward Proxy decryption. The following table describes the parameters.

Session Features: Forward Proxy Server Certificate Settings	
RSA Key Size	Select one of the following: • **Defined by destination host** (default)—Select this option if you want the firewall to generate certificates based on the key that the destination server uses: • If the destination server uses an RSA 1,024-bit key, the firewall generates a certificate with that key size and an SHA1 hashing algorithm. • If the destination server uses a key size larger than 1,024 bits (for example, 2,048 bits or 4,096 bits), the firewall generates a certificate that uses a 2,048-bit key and SHA-256 algorithm. • **1024-bit RSA**—Select this option if you want the firewall to generate certificates that use an RSA 1,024-bit key and the SHA1 hashing algorithm regardless of the key size that the destination server uses. As of December 31, 2013, public certificate authorities (CAs) and popular browsers have limited support for X.509 certificates that use keys of fewer than 2,048 bits. In the future, depending on security settings, the browser might warn the user or block the SSL/TLS session entirely when presented with such keys. • **2048-bit RSA**—Select this option if you want the firewall to generate certificates that use an RSA 2,048-bit key and the SHA-256 hashing algorithm regardless of the key size that the destination server uses. Public CAs and popular browsers support 2,048-bit keys, which provide better security than the 1,024-bit keys.
ECDSA Key Size	Select one of the following: • **Defined by destination host** (default)—Select this option if you want the firewall to generate certificates based on the key that the destination server uses: • If the destination server uses an ECDSA 256-bit or 384-bit key, the firewall generates a certificate with that key size. • If the destination server uses a key size larger than 384 bits, the firewall generates a certificate that uses a 521-bit key. • **256-bit ECDSA**— Select this option if you want the firewall to generate certificates that use an ECDSA 256-bit key, regardless of the key size that the destination server uses. • **384-bit ECDSA**—Select this option if you want the firewall to generate certificates that use an ECDSA 384-bit key, regardless of the key size that the destination server uses.

VPN Session Settings

Select **Session**, and in VPN Session Settings, configure global settings related to the firewall establishing a VPN session. The following table describes the settings.

VPN Session Settings	Description
Cookie Activation Threshold	Specify a maximum number of IKEv2 half-open IKE SAs allowed per firewall, above which cookie validation is triggered. When the number of half-open IKE SAs exceeds the Cookie Activation Threshold, the Responder will request a cookie, and the Initiator must respond with an IKE_SA_INIT containing a cookie. If the cookie validation is successful, another SA session can be initiated. A value of 0 means that cookie validation is always on. The Cookie Activation Threshold is a global firewall setting and should be lower than the Maximum Half Opened SA setting, which is also global (range is 0 to 65535; default is 500).
Maximum Half Opened SA	Specify the maximum number of IKEv2 half-open IKE SAs that Initiators can send to the firewall without getting a response. Once the maximum is reached, the firewall will not respond to new IKE_SA_INIT packets (range is 1 to 65535; default is 65535).
Maximum Cached Certificates	Specify the maximum number of peer certificate authority (CA) certificates retrieved via HTTP that the firewall can cache. This value is used only by the IKEv2 Hash and URL feature (range is 1 to 4000; default is 500).

Device > Setup > DLP

- **Device** > **Setup** > **DLP**

Configure the network settings for files scanned to the Enterprise Data Loss Prevention (DLP) cloud service.

Field	Description
Max Latency (sec)	Specify the maximum latency in seconds (between **1** and **240**) for a file upload before an action is taken by the firewall. Default is **60**.
Action on Max Latency	Specify the action the firewall takes when a file upload latency reaches the configured **Max Latency**. • **Allow** (default)— Firewall allows a file upload to continue to the DLP cloud service when the maximum latency is reached. • **Block**—Firewall blocks a file upload to the DLP cloud service that reaches the configured maximum latency.
Max File Size (MB)	Enforce a maximum file size (between **1** and **20**) for upload to the DLP cloud service. Default is **20**.
Action on Max File Size	Specify the action the firewall takes when a file upload reaches the configured **Max File Sized**. • **Allow** (default)— Firewall allows a file upload to continue to the DLP cloud service if the file is the configured maximum file size. • **Block**—Firewall blocks a file upload to the DLP cloud service if the file is the configured maximum file size.
Log Files Not Scanned	Check (enable) to generate an alert in the data filtering log when a file could not be uploaded to the DLP cloud service.
Action on any Error	Specify the action the firewall takes when an error is encountered during a file upload to the DLP cloud service. • **Allow** (default)— Firewall allows a file upload to continue to the DLP cloud service if an error is encountered during upload. • **Block**—Firewall blocks a file upload to the DLP cloud service if an error is encountered during upload.

Device > High Availability

- Device > High Availability

For redundancy, deploy your Palo Alto Networks next-generation firewalls in a high availability configuration of HA pairs or an HA cluster. When two HA firewalls function as an HA pair, there are two HA deployments:

- active/passive—In this deployment, the active peer continuously synchronizes its configuration and session information with the passive peer over two dedicated interfaces. In the event of a hardware or software disruption on the active firewall, the passive firewall becomes active automatically without loss of service. Active/passive HA deployments are supported with all interface modes: virtual-wire, Layer 2 or Layer 3.
- active/active—In this deployment, both HA peers are active and processing traffic. Such deployments are most suited for scenarios involving asymmetric routing or in cases where you want to allow dynamic routing protocols (OSPF, BGP) to maintain active status across both peers. Active/active HA is supported only in the virtual-wire and Layer 3 interface modes. In addition to the HA1 and HA2 links, active/active deployments require a dedicated HA3 link. HA3 link is used as packet forwarding link for session setup and asymmetric traffic handling.

In an HA pair, both peers must be of the same model, must be running the same PAN-OS and Content Release version, and must have the same set of licenses.

In addition, for the VM-Series firewalls, both peers must be on the same hypervisor and must have the same number of CPU cores allocated on each peer.

On supported firewall models, you can create a cluster of HA firewalls for session survivability within and between data centers. If a link goes down, the sessions fail over to a different firewall in the cluster. Such synchronization is helpful in use cases where HA peers are spread across multiple data centers or they are spread between an active data center and a standby data center. Another use case is horizontal scaling, where you add HA cluster members to a single data center to scale security and ensure session survivability. HA pairs can belong to an HA cluster and they count as two firewalls in the cluster. The number of firewalls supported in an HA cluster depends on the firewall model.

Important Considerations for Configuring HA

The following are important considerations for configuring an HA pair.

- The subnet that is used for the local and peer IP should not be used anywhere else on the virtual router.
- The OS and Content Release versions should be the same on each firewall. A mismatch can prevent peer firewalls from synchronizing.
- The LEDs are green on the HA ports for the active firewall and amber on the passive firewall.
- To compare the configuration of the local and peer firewalls, using the **Config Audit** tool on the **Device** tab by selecting the desired local configuration in the left selection box and the peer configuration in the right selection box.
- Synchronize the firewalls from the web interface by clicking **Push Configuration** in the HA widget on the **Dashboard**. The configuration on the firewall from which you push the configuration overwrites the

configuration on the peer firewall. To synchronize the firewalls from the CLI on the active firewall, use the command request high-availability sync-to-remote running-config.

In a High Availability (HA) active/passive configuration with firewalls that use 10 gigabit SFP+ ports, when a failover occurs and the active firewall changes to a passive state, the 10 gigabit Ethernet port is taken down and then brought back up to refresh the port, but does not enable transmit until the firewall becomes active again. If you have monitoring software on the neighboring device, it will see the port as flapping because it is going down and then up again. This is different behavior than the action with other ports, such as the 1 gigabit Ethernet port, which is disabled and still allows transmit, so flapping is not detected by the neighboring device.

HA General Settings

- Device > High Availability > General

To configure high availability (HA) pairs or HA cluster members, begin by selecting **Device** > **High Availability** > **General** and configuring the general settings.

HA Settings	Description
General Tab	
HA Pair Settings—Setup	**Enable HA Pair** to activate HA pair functionality and to access the following settings: • **Group ID**—Enter a number to identify the HA pair (1 to 63). This field is required (and must be unique) if multiple HA pairs reside on the same broadcast domain. • **Description**—(Optional) Enter a description for the HA pair. • **Mode**—Set the type of HA deployment: **Active Passive** or **Active Active**. • **Device ID**—In active/active configuration, set the Device ID to determine which peer will be active-primary (set **Device ID** to **0**) and which will be active-secondary (set the **Device ID** to **1**). • **Enable Config Sync**—Select this option to enable synchronization of configuration settings between the peers. *Enable config sync so that both devices always have the same configuration and process traffic the same way.* • **Peer HA1 IP Address**—Enter the IP address of the HA1 interface of the peer firewall. • **Backup Peer HA1 IP Address**—Enter the IP address for the peer's backup control link. *Configure a backup Peer HA1 IP Address so that, if the primary link fails, the backup link keeps the firewalls in sync and up to date.*
Active/Passive Settings	• **Passive Link State**—Select one of the following options to specify whether the data links on the passive firewall should remain up. This option is not available in the VM-Series firewall in AWS.

HA Settings	Description
	• **Shutdown**—Forces the interface link to the down state. This is the default option, which ensures that loops are not created in the network. • **Auto**—The links that have physical connectivity remain physically up but in a disabled state; they do not participate in ARP learning or packet forwarding. This will help in convergence times during the failover as the time to bring up the links is saved. In order to avoid network loops, do not select this option if the firewall has any Layer 2 interfaces configured. *If the firewall has no Layer 2 interfaces configured, set the Passive Link State to auto.* • **Monitor Fail Hold Down Time (min)**—Number of minutes a firewall will be in a non-functional state before becoming passive (range is 1 to 60). This timer is used when there are missed heartbeats or hello messages due to a link or path monitoring failure.
Election Settings	Specify or enable the following settings: • **Device Priority**—Enter a priority value to identify the active firewall. The firewall with the lower value (higher priority) becomes the active firewall (range is 0 to 255) when the preemptive capability is enabled on both firewalls in the pair. • **Preemptive**—Enables the higher priority firewall to resume active (active/passive) or active-primary (active/active) operation after recovering from a failure. You must enable the Preemption option on both firewalls for the higher priority firewall to resume active or active-primary operation upon recovery after a failure. If this setting is disabled, then the lower priority firewall remains active or active-primary even after the higher priority firewall recovers from a failure. *Whether to enable the Preemptive option depends on your business requirements. If you require the primary device to be the active device, enable Preemptive so that—after recovering from a failure—the primary device preempts the secondary device. If you require the fewest failover events, disable the Preemptive option so that—after a failover—the HA pair doesn't failover again to make the higher priority firewall the primary firewall.* • **Heartbeat Backup**—Uses the management ports on the HA firewalls to provide a backup path for heartbeat and hello messages. The management port IP address will be shared with the HA peer through the HA1 control link. No additional configuration is required. *Enable Heartbeat Backup if you use an in-band port for the HA1 and HA1 Backup links. Don't enable Heartbeat Backup if you use the management port for the HA1 or HA1 Backup links.*
	• **HA Timer Settings**—Select one of the preset profiles:

HA Settings	Description
	• **Recommended**: Use for typical failover timer settings. Unless you're sure that you need different settings, the best practice is to use the **Recommended** settings. • **Aggressive**: Use for faster failover timer settings.  *To view the preset value for an individual timer included in a profile, select Advanced and Load Recommended or Load Aggressive. The preset values for your hardware model will be displayed on-screen.* • **Advanced**: Allows you to customize the values to suit your network requirement for each of the following timers: • **Promotion Hold Time (ms)**—Number of milliseconds that the passive peer (in active/passive mode) or the active-secondary peer (in active/active mode) will wait before taking over as the active or active-primary peer after communications with the HA peer have been lost. This hold time begins only after the peer failure declaration. • **Hello Interval (ms)**—Number of milliseconds between the hello packets sent to verify that the HA program on the other firewall is operational (range is 8,000 to 60,000; default is 8,000). • **Heartbeat Interval (ms)**—Specify how frequently the HA peers exchange heartbeat messages in the form of an ICMP ping (range is 1,000 to 60,000; there is no default).
	• **Flap Max**—A flap is counted when the firewall leaves the active state within 15 minutes after it last left the active state. Specify the maximum number of flaps that are permitted before the firewall is determined to be suspended and the passive firewall takes over (range is 0 to 16; default is 3). The value 0 means there is no maximum (an infinite number of flaps is required before the passive firewall takes over). • **Preemption Hold Time (min)**—Number of minutes that a passive or active-secondary peer waits before taking over as the active or active-primary peer (range is 1 to 60; default is 1). • **Monitor Fail Hold Up Time (ms)**—Time interval, in milliseconds, during which the firewall will remain active following a path monitor or link monitor failure. This setting is recommended to avoid an HA failover due to the occasional flapping of neighboring devices (range is 0 to 60,000; default is 0). • **Additional Master Hold Up Time (ms)**—Additional time, in milliseconds, applied to the same event as the Monitor Fail Hold Up Time (range is 0 to 60,000; default is 500). The additional time interval is applied only to the active peer in active/passive mode and to the active-primary peer in active/active mode. This timer is recommended to avoid a failover when both peers experience the same link or path monitor failure simultaneously.
SSH HA Profile Setting	A type of SSH service profile that applies to the SSH sessions for the high availability (HA) appliances on your network. To apply an existing HA profile, select a profile, click **OK**, and **Commit** your change.  *You must perform an SSH service restart from your CLI to activate the profile.*

HA Settings	Description
	For more information, see Device > Certificate Management > SSH Service Profile.
Clustering Settings	**Enable Cluster Participation** to access the clustering settings. Firewalls that support HA clustering allow clusters of member firewalls (individuals or HA pairs where each firewall in a pair counts toward the total). The number of members per cluster that a firewall model supports is as follows: • PA-3200 Series: 6 members • PA-5200 Series: 16 members • PA-7080 Series: 4 members • PA-7050 Series: 6 members Configure the cluster: • **Cluster ID**—A unique numeric ID for an HA cluster in which all members can share session state (range is 1 to 99; there is no default). • **Cluster Description**—Short helpful description for the cluster. • **Cluster Synchronization Timeout (min)**—Maximum number of minutes that the local firewall waits before going to Active state when another cluster member (for example, in unknown state) is preventing the cluster from fully synchronizing (range is 0 to 30; default is 0). • **Monitor Fail Hold Down Time (min)**—Number of minutes after which a down link is retested to see if it is back up (range is 1 to 60; default is 1).
Operational Commands	
Suspend local device (or Make local device functional)	To place the local HA peer into a suspended state and temporarily disable HA functionality on it, use the following CLI operational command: • **`request high-availability state suspend`** To place the suspended local HA peer back into a functional state, use the CLI operational command: • **`request high-availability state functional`** To test failover, you can uncable the active (or active-primary) firewall.

HA Communications

- Device > High Availability > HA Communications

To configure HA links for HA pairs or HA clustering, select **Device** > **High Availability** > **HA Communications**.

HA Links	Description
Control Link (HA1)/Control Link (HA1 Backup)	The firewalls in an HA pair use HA links to synchronize data and maintain state information. Some firewall models have a dedicated Control Link and dedicated backup Control Link; for example, PA-5200 Series firewalls have HA1-A and HA1-B. In this case, you should enable the Heartbeat Backup option in the Elections Settings. If you are using a dedicated HA1 port for the Control Link HA

HA Links	Description
	link and a data port for Control Link (HA Backup), it is recommended that you enable the Heartbeat Backup option. For firewalls that do not have a dedicated HA port, such as the PA-220 firewall, you should configure the management port for the Control Link HA connection and a data port interface configured with type HA for the Control Link HA1 Backup connection. Because the management port is used in this case, there is no need to enable the Heartbeat Backup option because the heartbeat backups will already occur through the management interface connection. On the VM-Series firewall in AWS, the management port is used as the HA1 link. *When using a data port for the HA control link, keep in mind that because the control messages have to communicate from the dataplane to the management plane, if a failure occurs in the dataplane, peers cannot communicate HA control link information and a failover will occur. It is best to use the dedicated HA ports, or on firewalls that do not have a dedicated HA port, use the management port.*
Control Link (HA1)/Control Link (HA1 Backup)	Specify the following settings for the primary and backup HA control links: • **Port**—Select the HA port for the primary and backup HA1 interfaces. The backup setting is optional. • **IPv4/IPv6 Address**—Enter the IPv4 or IPv6 address of the HA1 interface for the primary and backup HA1 interfaces. The backup setting is optional. *PA-3200 Series firewalls don't support an IPv6 address for backup HA1 interfaces; use an IPv4 address.* • **Netmask**—Enter the network mask for the IP address (such as 255.255.255.0) for the primary and backup HA1 interfaces. The backup setting is optional. • **Gateway**—Enter the IP address of the default gateway for the primary and backup HA1 interfaces. The backup setting is optional. • **Link Speed**—(Models with dedicated HA ports only) Select the speed for the control link between the firewalls for the dedicated HA1 port. • **Link Duplex**—(Models with dedicated HA ports only) Select a duplex option for the control link between the firewalls for the dedicated HA1 port. • **Encryption Enabled**—Enable encryption after exporting the HA key from the HA peer and importing it onto this firewall. The HA key on this firewall must also be exported from this firewall and imported on the HA peer. Configure this setting for the primary HA1 interface. Import/export keys on the Certificates page (see Device > Certificate Management > Certificate Profile). *Enable encryption when firewalls aren't directly connected (HA1 connections go through network devices that can inspect, process, or capture traffic).* • **Monitor Hold Time (ms)**—Enter the length of time, in milliseconds, that the firewall will wait before declaring a peer failure due to a control link failure (range is 1,000 to 60,000; default is 3,000). This option monitors the physical link status of HA1 ports.
Data Link (HA2)	Specify the following settings for the primary and backup data link:

HA Links	Description
When an HA2 backup link is configured, failover to the backup link will occur if there is a physical link failure. With the HA2 keep-alive option enabled, the failover will also occur if the HA keep-alive messages fail based on the defined threshold.	• **Port**—Select the HA port. Configure this setting for the primary and backup HA2 interfaces. The backup setting is optional. • **IP Address**—Specify the IPv4 or IPv6 address of the HA interface for the primary and backup HA2 interfaces. The backup setting is optional. • **Netmask**—Specify the network mask for the HA interface for the primary and backup HA2 interfaces. The backup setting is optional. • **Gateway**—Specify the default gateway for the HA interface for the primary and backup HA2 interfaces. The backup setting is optional. If the HA2 IP addresses of the firewalls are in the same subnet, the Gateway field should be left blank. • **Enable Session Synchronization**—Enable synchronization of the session information with the passive firewall, and choose a transport option. *Enable session synchronization so that the secondary device has the session in its dataplane, which allows the firewall to match packets to the synchronized session and quickly forward packets. If you don't enable session synchronization, the firewall must create the session again, which introduces latency and could drop connections.*
	• **Transport**—Choose one of the following transport options: • **Ethernet**—Use when the firewalls are connected back-to-back or through a switch (Ethertype 0x7261). • **IP**—Use when Layer 3 transport is required (IP protocol number 99). • **UDP**—Use to take advantage of the fact that the checksum is calculated on the entire packet rather than just the header, as in the IP option (UDP port 29281). The benefit of using UDP mode is the presence of the UDP checksum to verify the integrity of a session sync message.

HA Links	Description
	• (Models with dedicated HA ports only) **Link Speed**—Select the speed for the control link between peers for the dedicated HA2 port. • (Models with dedicated HA ports only) **Link Duplex**—Select a duplex option for the control link between peers for the dedicated HA2 port. • **HA2 Keep-alive**—It is a best practice to select this option to monitor the health of the HA2 data link between HA peers. This option is disabled by default and you can enable it on one or both peers. If enabled, the peers will use keep-alive messages to monitor the HA2 connection to detect a failure based on the **Threshold** you set (default is 10,000 ms). If you enable HA2 keep-alive, the HA2 Keep-alive recovery Action will be taken. Select an **Action**: • **Log Only**—Logs the failure of the HA2 interface in the system log as a critical event. Select this option for active/passive deployments because the active peer is the only firewall forwarding traffic. The passive peer is in a backup state and is not forwarding traffic; therefore a split datapath is not required. If you have not configured any HA2 Backup links, state synchronization will be turned off. If the HA2 path recovers, an informational log will be generated. • **Split Datapath**—Select this option in active/active HA deployments to instruct each peer to take ownership of their local state and session tables when it detects an HA2 interface failure. Without HA2 connectivity, no state and session synchronization can happen; this action allows separate management of the session tables to ensure successful traffic forwarding by each HA peer. To prevent this condition, configure an HA2 Backup link. • **Threshold (ms)**—The duration in which keep-alive messages have failed before one of the above actions is triggered (range is 5,000 to 60,000; default is 10,000.
Clustering Links	Configure settings for HA4 links, which are dedicated HA cluster links that synchronize session state among all cluster members having the same cluster ID. The HA4 link between cluster members detects connectivity failures between cluster members. • **Port**—Select an HA interface to be the HA4 link (for example, ethernet1/1). • **IPv4/IPv6 Address**—Enter the IP address of the local HA4 interface. • **Netmask**—Enter the netmask. • **HA4 Keep-alive Threshold (ms)**—Length of time within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional (range is 5,000 to 60,000; default is 10,000). Configure HA4 Backup settings: • **Port**—Select an HA interface to be the HA4 backup link. • **IPv4/IPv6 Address**—Enter the address of the local HA4 backup link. • **Netmask**—Enter the netmask.

HA Link and Path Monitoring

- Device > High Availability > Link and Path Monitoring

To define HA failover conditions, configure HA link and path monitoring; select **Device** > **High Availability** > **Link and Path Monitoring**.

Link monitoring and path monitoring are not available for the VM-Series firewall in AWS.

HA Link and Path Monitoring Settings	Description
Link Monitoring	Specify the following: • **Enabled**—Enable link monitoring. Link monitoring allows failover to be triggered when a physical link or group of physical links fails. • **Failure Condition**—Select whether a failover occurs when any or all of the monitored link groups fail. *Enable and configure either path monitoring or link monitoring to help trigger a failover if a path or link goes down. Configure at least one Path Group for path monitoring and configure at least one Link Group for Link Monitoring.*
Link Groups	Define one or more link groups to monitor specific Ethernet links. To add a link group, specify the following and click **Add**: • **Name**—Enter a link group name. • **Enabled**—Enable the link group. • **Failure Condition**—Select whether a failure occurs when any or all of the selected links fail. • **Interfaces**—Select one or more Ethernet interfaces to be monitored.
Path Monitoring	Specify the following: • **Enabled**—Enable path monitoring based on the combined or independent Virtual Wire path monitoring, VLAN path monitoring, and Virtual Router* path monitoring. Path monitoring enables the firewall to monitor specified destination IP addresses by sending ICMP ping messages to make sure that they are responsive. Use path monitoring for virtual wire, Layer 2, or Layer 3 configurations where monitoring of other network devices is required for failover and link monitoring alone is not sufficient. • **Failure Condition**: • **Any**—(default) Firewall triggers an HA failover when path monitoring for a virtual wire or a VLAN or a virtual router* fails. • **All**—Firewall triggers an HA failover when path monitoring for a virtual wire and a VLAN and a virtual router* fails (whichever of the three are enabled). ** If you have Advanced Routing enabled, Logical Router replaces Virtual Router, and you can enable Logical Router Path Monitoring.* *Enable and configure either path monitoring or link monitoring to help trigger a failover if a path or link goes down. Configure at least one Path Group for path monitoring and configure at least one Link Group for Link Monitoring.*
Path Group	Define one or more path groups to monitor specific destination addresses for the interface type. **Add Virtual Wire Path**, and **Add VLAN Path**, and **Add Virtual**

HA Link and Path Monitoring Settings	Description
	Router Path. (If you have Advanced Routing enabled, you can **Add Logical Router Path**). For each type of path monitoring that you add, specify the following: • **Name**—Select virtual wire, VLAN, or virtual router* to monitor (drop-down choices are based on path monitoring type you are adding). • **Source IP**—For virtual wire and VLAN interfaces, enter the source IP address to use in the pings sent to the next-hop router (Destination IP address). The local router must be able to route the address to the firewall. (The source IP address for path groups associated with virtual routers* will be automatically configured as the interface IP address that is indicated in the route table as the egress interface for the specified destination IP address.) • **Enabled**—Enable monitoring of virtual wire, VLAN, or virtual router*. • **Failure Condition**: • **Any** (default)—Firewall determines virtual wire, VLAN, or virtual router* has failed when a ping failure in any destination IP group occurs. • **All**—Firewall determines the virtual wire, VLAN, or virtual router* has failed when a ping failure in all destination IP groups occurs. *The actual HA failover is determined by the Failure Condition you set for Path Monitoring, which considers virtual wire, VLAN, and virtual router* path monitoring (whichever you enabled).* • **Ping Interval**—Specify the interval between pings that are sent to the destination IP address (range is 200 to 60,000ms; default is 200ms). • **Ping Count**—Specify the number of failed pings before declaring a failure (range is 3 to 10; default is 10). ** If you have Advanced Routing enabled, Logical Router replaces Virtual Router, and you can enable Logical Router Path Monitoring.*
Destination IP for Path Group	• **Destination IP**—**Add** one or more destination IP address groups to monitor for the path group. • **Destination IP Group**—Enter a name for the group. • **Add** one or more **Destination IP** addresses to monitor for the group. • **Enabled**—Select to enable the Destination IP group. • **Failure Condition**: Select **Any** (to specify that if a ping failure occurs for any IP address in the group, the destination group is considered to have failed) or **All** (to specify that if a ping failure occurs for all IP addresses in the group, the destination group is considered to have failed).

HA Active/Active Config

- Device > High Availability > Active/Active Config

To configure settings for an Active/Active HA pair, select **Device** > **High Availability** > **Active/Active Config**.

Active/Active Config Settings	Description
Packet Forwarding	**Enable** peers to forward packets over the HA3 link for session setup and for Layer 7 inspection (App-ID, Content-ID, and threat inspection) of asymmetrically routed sessions.
HA3 Interface	Select the data interface you plan to use to forward packets between active/active HA peers. The interface you use must be a dedicated Layer 2 interface set to Interface Type **HA**.  *If the HA3 link fails, the active-secondary peer will transition to the non-functional state.To prevent this condition, configure a Link Aggregation Group (LAG) interface with two or more physical interfaces as the HA3 link. The firewall does not support an HA3 Backup link. An aggregate interface with multiple interfaces will provide additional capacity and link redundancy to support packet forwarding between HA peers.* You must enable jumbo frames on the firewall and on all intermediary networking devices when using the HA3 interface. To enable jumbo frames, select **Device** > **Setup** > **Session** and select the option to **Enable Jumbo Frame** in the Session Settings section.
VR Sync	Force synchronization of all virtual routers configured on the HA peers. Use this option when the virtual router is not configured for dynamic routing protocols. Both peers must be connected to the same next-hop router through a switched network and must use static routing only.
QoS Sync	Synchronize the QoS profile selection on all physical interfaces. Use this option when both peers have similar link speeds and require the same QoS profiles on all physical interfaces. This setting affects the synchronization of QoS settings on the **Network** tab. QoS policy is synchronized regardless of this setting.
Tentative Hold Time (sec)	When a firewall in an HA active/active configuration fails, it will go into a tentative state. The transition from tentative state to active-secondary state triggers the Tentative Hold Time, during which the firewall attempts to build routing adjacencies and populate its route table before it will process any packets. Without this timer, the recovering firewall would enter the active-secondary state immediately and would silently discard packets because it would not have the necessary routes (default is 60 seconds).
Session Owner Selection	The session owner is responsible for all Layer 7 inspection (App-ID and Content-ID) for the session and for generating all Traffic logs for the session. Select one of the following options to specify how to determine the session owner for a packet: • **First packet**—Select this option to designate the firewall that receives the first packet in a session as the session owner. This is the best practice configuration to minimize traffic across HA3 and distribute the dataplane load across peers. • **Primary Device**—Select this option if you want the active-primary firewall to own all sessions. In this case, if the active-secondary firewall receives the first

Active/Active Config Settings	Description
	packet, it will forward all packets requiring Layer 7 inspection to the active-primary firewall over the HA3 link.
Virtual Address	Click **Add**, select the **IPv4** or **IPv6** tab and then click **Add** again to enter options to specify the type of HA virtual address to use: Floating or ARP Load Sharing. You can also mix the type of virtual address types in the pair. For example, you could use ARP load sharing on the LAN interface and a Floating IP on the WAN interface. • **Floating**—Enter an IP address that will move between HA peers in the event of a link or system failure. Configure two floating IP addresses on the interface, so that each firewall will own one and then set the priority. If either firewall fails, the floating IP address transitions to the HA peer. • **Device 0 Priority**—Set the priority for the firewall with Device ID 0 to determine which firewall will own the floating IP address. A firewall with the lowest value will have the highest priority. • **Device 1 Priority**—Set the priority for the firewall with Device ID 1 to determine which firewall will own the floating IP address. A firewall with the lowest value will have the highest priority. • **Failover address if link state is down**—Use the failover address when the link state is down on the interface. • **Floating IP bound to the Active-Primary HA device**—Select this option to bind the floating IP address to the active-primary peer. In the event one peer fails, traffic is sent continuously to the active-primary peer even after the failed firewall recovers and becomes the active-secondary peer.
Virtual Address (cont)	• **ARP Load Sharing**—Enter an IP address that will be shared by the HA pair and provide gateway services for hosts. This option is only required if the firewall is on the same broadcast domain as the hosts. Select the **Device Selection Algorithm**: • **IP Modulo**—Select the firewall that will respond to ARP requests based on the parity of the ARP requesters IP address. • **IP Hash**—Select the firewall that will respond to ARP requests based on a hash of the ARP requesters IP address.

Cluster Config

- Device > High Availability > Cluster Config

Add members to an HA cluster by selecting **Device** > **High Availability** > **Cluster Config**.

Cluster Config	Description
Add	**Add** a cluster member. You must add the local firewall and if you are using HA pairs, you must add both HA peers of the pair as cluster members. • (Supported firewalls) **Device Serial Number**—Enter the unique serial number of the cluster member. • (Panorama) **Device**—Select a device from the dropdown and enter a **Device Name**.

Cluster Config	Description
	• **HA4 IP Address**—Enter the IP address of the HA4 link for the cluster member. • **HA4 Backup IP Address**—Enter the IP address of the backup HA4 link for the cluster member. • **Session Synchronization**—Select to enable session synchronization with this cluster member. • **Description**—Enter helpful description.
Delete	Select one or more cluster members and **Delete** them from the cluster.
Enable	(Supported firewalls) You can determine whether or not a cluster member synchronizes sessions with other members. By default, all members are allowed to synchronize sessions. If you disable synchronization for one or more members, select **Enable** to re-enable synchronization for one or more members.
Disable	(Supported firewalls) Select one or more members and **Disable** synchronization with other members.
Refresh	(Panorama) Select **Refresh** to refresh the list of HA devices in the HA cluster.

Device > Log Forwarding Card

- Device > Log Forwarding Card

The Log Forwarding Card (LFC) is a high-performance log card that forwards all dataplane logs (traffic and threat for example) from the firewall to one or more external logging systems, such as Panorama or a syslog server. Because the dataplane logs are no longer available on the local firewall, the ACC tab is removed from the management web interface and Monitor > Logs contain only management logs (Configuration, System, and Alarms).

You need to configure the ports for the LFC. Port 1 operates at 10Gbps and Port 9 operates at 40Gbps. Configure the ports in **Device > Log Forwarding Card**. The firewall uses these ports to forward all dataplane logs to an external system, such as Panorama or a syslog server.

See the PA-7000 Series Hardware Reference Guide for information about the LFC requirements and components.

For an LFC interface, configure the settings described in the following table.

LFC Interface Settings	Description
Name	Enter an interface name. For an LFC, you must select **lfc1/1** or **lfc1/9**.
Comment	Enter an optional description for the interface.
IPv4	If your network uses IPv4, define the following: • **IP address**—The IPv4 address of the port. • **Netmask**—The network mask for the IPv4 address of the port. • **Default Gateway**—The IPv4 address of the default gateway for the port.
IPv6	If your network uses IPv6, define the following: • **IP address**—The IPv6 address of the port. • **Default Gateway**—The IPv6 address of the default gateway for the port.
Link Speed	Select the interface speed in Mbps (**10000** or **40000**), or select **auto** (default) to have the firewall automatically determine the speed based on the connection. The interface speed available is dependent on the port used (lfc1/1 or lfc1/9). For interfaces that have a non-configurable speed, **auto** is the only option.
Link State	Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically based on the connection (**auto**). The default is **auto**.
LACP Port Priority	The firewall only uses this field if you enabled Link Aggregation Control Protocol (LACP) for the aggregate group. If the number of interfaces you assign to the group exceeds the number of active interfaces (the Max Ports field), the firewall uses the LACP port priorities of the interfaces to determine which are in standby mode. The lower the numeric value, the higher the priority (range is 1-65,535; default is 32,768).

Subinterfaces are available if you have multi-vsys enabled. To configure an LFC subinterface, add a subinterface and use the setting described in the following table.

LFC Subinterface Settings	Description
Interface Name	**Interface Name** (read-only) displays the name of the log card interface you selected. In the adjacent field, enter a numeric suffix (1-9,999) to identify the subinterface.
Comment	Enter an optional description for the interface.
Tag	Enter the VLAN **Tag** (0-4,094) for the subinterface.  *Make the tag the same as the subinterface number for ease of use.*
Virtual System	Select the virtual system (vsys) to which the Log Forwarding Card (LFC) subinterface is assigned. Alternatively, you can click **Virtual Systems** to add a new vsys. Once an LFC subinterface is assigned to a vsys, that interface is used as the source interface for all services that forward logs (syslog, email, SNMP) from the log card.
IPv4	If your network uses IPv4, define the following: • **IP address**—The IPv4 address of the port. • **Netmask**—The network mask for the IPv4 address of the port. • **Default Gateway**—The IPv4 address of the default gateway for the port.
IPv6	If your network uses IPv6, define the following: • **IP address**—The IPv6 address of the port. • **Default Gateway**—The IPv6 address of the default gateway for the port.

Device > Config Audit

Select **Device** > **Config Audit** to see the differences between configuration files. The page displays the configurations side by side in separate panes and highlights the differences line by line using colors to indicate additions (green), modifications (yellow), or deletions (red):

Config Audit Settings	Description
Configuration name drop-downs (unlabeled)	Select two configurations to compare in the (unlabeled) configuration name drop-downs (the defaults are **Running config** and **Candidate config**). *You can filter a drop-down by entering a text string derived from the Description value of the commit operation associated with the desired configuration (see Commit Changes).*
Context drop-down	Use the **Context** drop-down to specify the number of lines to display before and after the highlighted differences in each file. Specifying more lines can help you correlate the audit results to settings in the web interface. If you set the **Context** to **All**, the results include the entire configuration files.
Go	Click **Go** to start the audit.
Previous (‹‹) and Next (››)	These navigation arrows are enabled when consecutive configuration versions are selected in the configuration name drop-downs. Click ‹‹ to compare the previous pair of configurations in the drop-downs or click ›› to compare the next pair of configurations.

Device > Password Profiles

- Device > Password Profiles
- Panorama > Password Profiles

Select **Device** > **Password Profiles** or **Panorama** > **Password Profiles** to set basic password requirements for individual local accounts. Password profiles override any Minimum Password Complexity settings you defined for all local accounts (**Device** > **Setup** > **Management**).

To apply a password profile to an account, select **Device** > **Administrators** (firewalls) or **Panorama** > **Administrators** (Panorama), select an account, and then select the **Password Profile**.

You cannot assign password profiles to administrative accounts that use local database authentication (see Device > Local User Database > Users).

To create a password profile, **Add** and specify the information in the following table.

Password Profile Settings	Description
Name	Enter a name to identify the password profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Required Password Change Period (days)	Require that administrators change their password on a regular basis specified a by a number of days (range is 0 to 365). Example, if the value is set to 90, administrators will be prompted to change their password every 90 days. You can also set an expiration warning from 0 to 30 days and specify a grace period.
Expiration Warning Period (days)	If a required password change period is set, this setting can be used to prompt the user to change their password at each log in as the forced password change date approaches (range is 0 to 30).
Post Expiration Admin Login Count	Allow the administrator to log in a specified number of times after their account has expired. Example, if the value is set to 3 and their account has expired, they can log in 3 more times before their account is locked out (range is 0 to 3).
Post Expiration Grace Period (days)	Allow the administrator to log in the specified number of days after their account has expired (range is 0 to 30).

Username and Password Requirements

The following table lists the valid characters that can be used in usernames and passwords for PAN-OS and Panorama accounts.

Account Type	Username and Password Restrictions
Password Character Set	There are no restrictions on any password field character sets.

Account Type	Username and Password Restrictions
Remote Admin, SSL-VPN, or Authentication Portal	The following characters are not allowed for the username: • Backtick (`) • Angular brackets (< and >) • Ampersand (&) • Asterisk (*) • At sign (@) • Question mark (?) • Pipe (|) • Single-Quote (') • Semicolon (;) • Double-Quote (") • Dollar ($) • Parentheses ('(' and ')') • Colon (':')
Local Administrator Accounts	The following are the allowed characters for local usernames: • Lowercase (a-z) • Uppercase (A-Z) • Numeric (0-9) • Underscore (_) • Period (.) • Hyphen (-) *Login names cannot start with a hyphen (-).*

Device > Administrators

Administrator accounts control access to firewalls and Panorama. A firewall administrator can have full or read-only access to a single firewall or to a virtual system on a single firewall. Firewalls have a predefined **admin** account that has full access.

To define Panorama administrators, see Panorama > Managed Devices > Summary.

The following authentication options are supported:

- Password authentication—The administrator enters a username and password to log in. This authentication requires no certificates. You can use it in conjunction with authentication profiles, or for local database authentication.
- Client certificate authentication (web)—This authentication requires no username or password; the certificate suffices to authenticate access to the firewall.
- Public key authentication (SSH)—The administrator generates a public/private key pair on the machine that requires access to the firewall, and then uploads the public key to the firewall to allow secure access without requiring the administrator to enter a username and password.

To add an administrator, click **Add** and fill in the following information:

Administrator Account Settings	Description
Name	Enter a login name for the administrator (up to 31 characters). The name is case sensitive and must be unique. Use only letters, numbers, hyphens, periods, and underscores. Login names cannot start with a hyphen (-).
Authentication Profile	Select an authentication profile for administrator authentication. You can use this setting for RADIUS, TACACS+, LDAP, Kerberos, SAML, or local database authentication. For details, see Device > Authentication Profile.
Use only client certificate authentication (web)	Select this option to use client certificate authentication for web access. If you select this option, a username and password are not required; the certificate is sufficient to authenticate access to the firewall.
New Password Confirm New Password	Enter and confirm a case-sensitive password for the administrator (up to 31 characters). You can also select **Setup** > **Management** to enforce a minimum password length. *To ensure that the firewall management interface remains secure, we recommend that you periodically change administrative passwords using a mixture of lower-case letters, upper-case letters, and numbers. You can also configure* Minimum Password Complexity *settings for all administrators on the firewall.*

Administrator Account Settings	Description
Use Public Key Authentication (SSH)	Select this option to use SSH public key authentication. Click **Import Key** and browse to select the public key file. The uploaded key appears in the read-only text area. Supported key file formats are IETF SECSH and OpenSSH. Supported key algorithms are DSA (1,024 bits) and RSA (768 to 4,096 bits). *If the public key authentication fails, the firewall prompts the administrator for a username and password.*
Administrator Type	Assign a role to this administrator. The role determines what the administrator can view and modify. If you select **Role Based**, select a custom role profile from the drop-down. For details, see Device > Admin Roles. If you select **Dynamic**, you can select one of the following predefined roles: • **Superuser**—Has full access to the firewall and can define new administrator accounts and virtual systems. You must have superuser privileges to create an administrative user with superuser privileges. • **Superuser** (read-only)—Has read-only access to the firewall. • **Device administrator**—Has full access to all firewall settings except for defining new accounts or virtual systems. • **Device administrator** (read-only)—Has read-only access to all firewall settings except password profiles (no access) and administrator accounts (only the logged in account is visible). • **Virtual system administrator**—Has access to specific virtual systems on the firewall to create and manage specific aspects of virtual systems (if Multi Virtual System Capability is enabled). A virtual system administrator doesn't have access to network interfaces, virtual routers, IPSec tunnels, VLANs, virtual wires, GRE tunnels, DHCP, DNS Proxy, QoS, LLDP, or network profiles. • **Virtual system administrator** (read-only)—Has read-only access to specific virtual systems on the firewall to view specific aspects of virtual systems (if Multi Virtual System Capability is enabled). A virtual system administrator with read-only access doesn't have access to network interfaces, virtual routers, IPSec tunnels, VLANs, virtual wires, GRE tunnels, DHCP, DNS Proxy, QoS, LLDP, or network profiles.
Virtual System (Virtual system administrator role only)	Click **Add** to select the virtual systems that the administrator can manage.
Password Profile	Select the password profile, if applicable. To create a new password profile, see Device > Password Profiles.

Administrator Account Settings	Description
	 *Create a password profile for administrators to ensure that admin passwords expire after a configured time period. Changing admin passwords regularly helps prevent attackers from using saved or stolen credentials.*

Device > Admin Roles

Select **Device** > **Admin Roles** to define Admin Role profiles, which are custom roles that determine the access privileges and responsibilities of administrative users. You assign Admin Role profiles or dynamic roles when you create administrative accounts (Device>Administrators).

To define Admin Role profiles for Panorama administrators, see Panorama > Managed Devices > Summary.

The firewall has three predefined roles you can use for common criteria purposes. You first use the superuser role for initial firewall configuration and to create the administrator accounts for the Security Administrator, Audit Administrator, and Cryptographic Administrator. After you create these accounts and apply the proper common criteria Admin Roles, you then log in using those accounts. The default superuser account in Federal Information Processing Standard (FIPS)/Common Criteria (CC) FIPS-CC mode is **admin** and the default password is **paloalto**. In standard operating mode, the default **admin** password is **admin**. The predefined Admin Roles were created where there is no overlap in capabilities, except that all have read-only access to the audit trail (except audit administrator with full read/delete access. These admin roles cannot be modified and are defined as follows:

- auditadmin—The Audit Administrator is responsible for the regular review of the firewall's audit data.
- cryptoadmin—The Cryptographic Administrator is responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to the firewall.
- securityadmin—The Security Administrator is responsible for all other administrative tasks (such as creating Security policy) not addressed by the other two administrative roles.

To add an Admin Role profile, click **Add** and specify the settings described in the following table.

Create custom roles to limit administrator access to only what each type of administrator needs. For each type of administrator, enable, disable, or set read-only access for Web UI, XML API, Command Line, and REST API access.

Administrator Role Settings	
Name	Enter a name to identify this administrator role (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	(Optional) Enter a description for the role (up to 255 characters).
Role	Select the scope of administrative responsibility: • **Device**—The role applies to the entire firewall, regardless whether it has more than one virtual system (vsys). • **Virtual System**—The role applies to specific virtual systems on the firewall and specific aspects of virtual systems (if Multi Virtual System Capability is enabled). An Admin Role Profile based on **Virtual System** doesn't have access on the **Web UI** tab to Network Interfaces, VLANs, Virtual Wires, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, QoS, LLDP, or Network Profiles. You select the virtual systems when you create administrative accounts (Device>Administrators).
WebUI	Click the icons for specific web interface features to set the permitted access privileges:

Administrator Role Settings	
	• **Enable**—Read/write access to the selected feature. • **Read Only**—Read-only access to the selected feature. • **Disable**—No access to the selected feature.
XML API	Click the icons for specific XML API features to set the permitted access privileges (**Enable** or **Disable**).
Command Line	Select the type of role for CLI access. The default is **None**, which means access to the CLI is not permitted. The other options vary by Role scope: • **Device** • **superuser**—Has full access to the firewall and can define new administrator accounts and virtual systems. You must have superuser privileges to create an administrative user with superuser privileges. • **superreader**—Has read-only access to the firewall. • **deviceadmin**—Has full access to all firewall settings except for defining new accounts or virtual systems. • **devicereader**—Has read-only access to all firewall settings except password profiles (no access) and administrator accounts (only the logged in account is visible). • **Virtual System** • **vsysadmin**—Has access to specific virtual systems on the firewall to create and manage specific aspects of virtual systems. The **vsysadmin** setting doesn't control firewall-level or network-level functions (such as static and dynamic routing, IP addresses of interfaces, IPSec tunnels, VLANs, virtual wires, virtual routers, GRE tunnels, DHCP, DNS Proxy, QoS, LLDP, or network profiles). • **vsysreader**—Has read-only access to specific virtual systems on the firewall and specific aspects of a virtual system. The **vsysreader** setting doesn't have access to firewall-level or network-level functions (such as static and dynamic routing, IP addresses of interfaces, IPSec tunnels, VLANs, virtual wires, virtual routers, GRE tunnels, DHCP, DNS Proxy, QoS, LLDP, or network profiles).
REST API	Click the icons for specific REST API features to set the permitted access privileges (**Enable**, **Read Only**, or **Disable**).

Device > Access Domain

- Device > Access Domain

Configure access domains to restrict administrator access to specific virtual systems on the firewall. The firewall supports access domains only if you use a RADIUS, TACACS+, or SAML identity server (IdP) server to manage administrator authentication and authorization. To enable access domains, you must define:

- A server profile for the external authentication server—See Device > Server Profiles > RADIUS, Device > Server Profiles > TACACS+, and Device > Server Profiles > SAML Identity Provider.
- RADIUS Vendor-Specific Attributes (VSAs), TACACS+ VSAs, or SAML attributes.

When an administrator attempts to log in to the firewall, the firewall queries the external server for the access domain of the administrator. The external server returns the associated domain and the firewall then restricts the administrator to the virtual systems that you specified in the access domain. If the firewall does not use an external server for authenticating and authorizing administrators, the **Device** > **Access Domain** settings are ignored.

On Panorama, you can manage access domains locally or by using RADIUS VSAs, TACACS+ VSAs, or SAML attributes (see Panorama > Access Domains*).*

Access Domain Settings	Description
Name	Enter a name for the access domain (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, underscores, and periods.
Virtual Systems	Select virtual systems in the Available column and **Add** them. Access Domains are only supported on firewalls that support virtual systems.

Device > Authentication Profile

Use this page to configure settings for authenticating administrators and end users. The firewall and Panorama support local, RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0, and multi-factor authentication (MFA) services.

Create at least one Authentication profile to provide external authentication, which keeps all authentication requests in one place for easier management and uses a standard authentication process that includes services such as tracking. Best is to create and prioritize (Device > Authentication Sequence) multiple Authentication profiles using different methods in case of authentication failure, and to create at least one local login account to fall back on if all external methods fail.

You can also use this page to register a firewall or Panorama service (such as administrative access to the web interface) with a SAML identity provider (IdP). Registering the service enables the firewall or Panorama to use the IdP for authenticating users who request the service. You register a service by entering its SAML metadata on the IdP. The firewall and Panorama make registration easy by automatically generating a SAML metadata file based on the authentication profile that you assigned to the service; you can export this metadata file to the IdP.

- Authentication Profile
- SAML Metadata Export from an Authentication Profile

Authentication Profile

- Device > Authentication Profile

Select **Device** > **Authentication Profile** or **Panorama** > **Authentication Profile** to manage authentication profiles. To create a new profile, **Add** one and complete the following fields.

After configuring an authentication profile, use the ***`test authentication`*** *CLI command to determine whether the firewall or Panorama management server can communicate with the back-end authentication server and whether the authentication request succeeded. You can perform authentication tests on the candidate configuration to determine whether the configuration is correct before you commit.*

Authentication Profile Settings	Description
Name	Enter a name to identify the profile. The name is case-sensitive, can have up to 31 characters, and can include only letters, numbers, spaces, hyphens, underscores, and periods. The name must be unique in the current **Location** (firewall or virtual system) relative to other authentication profiles and to authentication sequences. *In a firewall that is in multiple virtual systems mode, if the Location of the authentication profile is a virtual system, don't enter the same name as an authentication sequence in the Shared location. Similarly, if the profile Location is Shared, don't enter the same name as a sequence in a virtual system. While you can commit an authentication profile and sequence with the same names in these cases, it can result in reference errors.*

Authentication Profile Settings	Description
Location	Select the scope in which the profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Authentication Tab The firewall invokes the authentication service that you configure in this tab before invoking any multi-factor authentication (MFA) services that you add in the Factors Tab. *If the firewall integrates with an MFA vendor through RADIUS instead of the vendor API, you must configure a RADIUS server profile for that vendor, not an MFA server profile.*	
Type	Select the type of service that provides the first (and optionally the only) authentication challenge that users see. Based on your selection, the dialog displays other settings that you define for the service. The options are: • **None**—Do not use any authentication. • **Local Database**—Use the local authentication database on the firewall. This option is not available on Panorama. • **RADIUS**—Use a Remote Authentication Dial-In User Service (RADIUS) server. • **TACACS+**—Use a Terminal Access Controller Access-Control System Plus (TACACS+) server. • **LDAP**—Use a Lightweight Directory Access Protocol (LDAP) server. • **Kerberos**—Use a Kerberos server. • **SAML**—Use a Security Assertion Markup Language 2.0 (SAML 2.0) identity provider (IdP). *Administrators can use SAML to authenticate to the firewall or Panorama web interface but not to the CLI.*
Server Profile (RADIUS, TACACS+, LDAP, or Kerberos only)	Select the authentication server profile from the drop-down. See Device > Server Profiles > RADIUS, Device > Server Profiles > TACACS+, Device > Server Profiles > LDAP, or Device > Server Profiles > Kerberos.
IdP Server Profile (SAML only)	Select the SAML Identity Provider server profile from the drop-down. See Device > Server Profiles > SAML Identity Provider.
Retrieve user group from RADIUS (RADIUS only)	Select this option to collect user group information from Vendor-Specific Attributes (VSAs) defined on the RADIUS server. The firewall uses the information to match authenticating users against Allow List entries, not for enforcing policies or generating reports.
Retrieve user group from TACACS+	Select this option to collect user group information from Vendor-Specific Attributes (VSAs) defined on the TACACS+ server. The firewall uses the

Authentication Profile Settings	Description
(TACACS+ only)	information to match authenticating users against Allow List entries, not for enforcing policies or generating reports.
Login Attribute (LDAP only)	Enter an LDAP directory attribute that uniquely identifies the user and functions as the login ID for that user.
Password Expiry Warning (LDAP only)	If the authentication profile is for GlobalProtect users, enter the number of days before password expiration to start displaying notification messages to users to alert them that their passwords are expiring in x number of days. By default, notification messages will display seven days before password expiry (range is 1 to 255). Users will not be able to access the VPN if their passwords expire. *Consider configuring the GlobalProtect agents to use the pre-logon connection method. This will enable users to connect to the domain to change their passwords even after the password has expired.* If users allow their passwords to expire, the administrator can assign a temporary LDAP password to enable users to log in to the VPN. In this workflow, we recommend setting the **Authentication Modifier** in the portal configuration to **Cookie authentication for config refresh** (otherwise, the temporary password will be used to authenticate to the portal, but the gateway login will fail, preventing VPN access).
Certificate for Signing Requests (SAML only)	Select the certificate that the firewall will use to sign SAML messages that it sends to the identity provider (IdP). This field is required if you enable the **Sign SAML Message to IdP** option in the **IdP Server Profile** (see Device > Server Profiles > SAML Identity Provider). Otherwise, selecting a certificate to sign SAML messages is optional. When generating or importing a certificate and its associated private key, the key usage attributes specified in the certificate control how you can use the key: • If the certificate explicitly lists key usage attributes, one of the attributes must be Digital Signature, which is not available in certificates that you generate on the firewall. In this case, you must Import the certificate and key from your enterprise certificate authority (CA) or a third-party CA. • If the certificate doesn't specify key usage attributes, you can use the key for any purpose, including signing messages. In this case, you can use any method to obtain the certificate and key for signing SAML messages. *Palo Alto Networks recommends using a signing certificate to ensure the integrity of SAML messages sent to the IdP.*
Enable Single Logout (SAML only)	Select this option to enable users to log out of every authenticated service by logging out of any single service. Single logout (SLO) applies only to services that users accessed through SAML authentication. The services can be external to your organization or internal (such as the firewall web interface). This option applies only if you entered an **Identity Provider SLO URL** in the IdP Server Profile. You cannot enable SLO for Authentication Portal users.

Authentication Profile Settings	Description
	After logging out users, the firewall automatically removes their IP address-to-username mappings.
Certificate Profile (SAML only)	Select the Certificate Profile that the firewall will use to validate: • The **Identity Provider Certificate** specified in the IdP Server Profile. The IdP uses this certificate to authenticate to the firewall. The firewall validates the certificate when you **Commit** the authentication profile configuration. • SAML messages that the IdP sends to the firewall for single sign-on (SSO) and single logout (SLO) authentication. The IdP uses the **Identity Provider Certificate** specified in the IdP Server Profile to sign the messages. See Device > Certificate Management > Certificate Profile.
User Domain and Username Modifier (All authentication types except SAML)	The firewall uses the **User Domain** for matching authenticating users against Allow List entries and for User-ID group mapping. You can specify a **Username Modifier** to modify the format of the domain and username that a user enters during login. The firewall uses the modified string for authentication. Select from the following options: • To send only the unmodified user input, leave the **User Domain** blank (default) and set the **Username Modifier** to the variable **%USERINPUT%** (default). • To prepend a domain to the user input, enter a **User Domain,** and set the **Username Modifier** to **%USERDOMAIN%\%USERINPUT%**. • To append a domain to the user input, enter a **User Domain** and set the **Username Modifier** to **%USERINPUT%@%USERDOMAIN%**. *If the Username Modifier includes the %USERDOMAIN% variable, the User Domain value replaces any domain string that the user enters. If you specify the %USERDOMAIN % variable and leave the User Domain blank, the firewall removes any user-entered domain string. The firewall resolves domain names to the appropriate NetBIOS name for User-ID group mapping. This applies to both parent and child domains. User Domain modifiers take precedence over automatically derived NetBIOS names.* • To allow the firewall to use the server profile type to determine how and when in the authentication sequence to modify the format of the user input, manually enter **None** as the **Username Modifier**. For more information on this option, refer to Configure an Authentication Profile and Sequence in the PAN-OS Administrator's Guide.
Kerberos Realm (All authentication types except SAML)	If your network supports Kerberos single sign-on (SSO), enter the **Kerberos Realm** (up to 127 characters). This is the hostname portion of the user login name. For example, the user account name user@EXAMPLE.LOCAL has realm EXAMPLE.LOCAL.
Kerberos Keytab	If your network supports Kerberos single sign-on (SSO), click **Import**, click **Browse** to locate the keytab file, and then click **OK**. A keytab contains Kerberos account information (principal name and hashed password) for the firewall,

Authentication Profile Settings	Description
(All authentication types except SAML)	which is required for SSO authentication. Each authentication profile can have one keytab. During authentication, the firewall first tries to use the keytab to establish SSO. If it succeeds and the user attempting access is in the Allow List, authentication succeeds immediately. Otherwise, the authentication process falls back to manual authentication (username/password) of the specified **Type**, which doesn't have to be Kerberos. *If the firewall is in FIPS/CC mode, the algorithm must be aes128-cts-hmac-sha1-96 or aes256-cts-hmac-sha1-96. Otherwise, you can also use des3-cbc-sha1 or arcfour-hmac. However, if the algorithm in the keytab does not match the algorithm in the service ticket that the Ticket Granting Service issues to clients to enable SSO, the SSO process fails. Your Kerberos administrator determines which algorithms the service tickets use.*
Username Attribute (SAML only)	Enter the SAML attribute that identifies the username of an authenticating user in messages from the IdP (default is **username**). If the **IdP Server Profile** contains metadata that specifies a username attribute, the firewall automatically populates this field with that attribute. The firewall matches usernames retrieved from SAML messages with users and user groups in the **Allow List** of the authentication profile. Because you cannot configure the firewall to modify the domain/username string that a user enters during SAML logins, the login username must exactly match an **Allow List** entry. This is the only SAML attribute that is mandatory. *SAML messages might display the username in the subject field. The firewall automatically checks the subject field if the username attribute doesn't display the username.*
User Group Attribute (SAML only)	Enter the SAML attribute that identifies the user group of an authenticating user in messages from the IdP (default is **usergroup**). If the **IdP Server Profile** contains metadata that specifies a user group attribute, the field automatically uses that attribute. The firewall uses the group information to match authenticating users against **Allow List** entries, not for policies or reports.
Admin Role Attribute (SAML only)	Enter the SAML attribute that identifies the administrator role of an authenticating user in messages from the IdP (default is **admin-role**). This attribute applies only to firewall administrators, not to end users. If the **IdP Server Profile** contains metadata that specifies an admin-role attribute, the firewall automatically populates this field with that attribute. The firewall matches its predefined (dynamic) roles or Admin Role profiles with the roles retrieved from SAML messages to enforce role-based access control. If a SAML message has multiple admin-role values for an administrator with only one role, matching applies only to the first (left-most) value in the admin-role attribute. For an administrator with more than one role, the matching can apply to multiple values in the attribute.
Access Domain Attribute	Enter the SAML attribute that identifies the access domain of an authenticating user in messages from the IdP (default is **access-domain**). This attribute applies only to firewall administrators, not to end users. If the **IdP Server Profile**

Authentication Profile Settings	Description
(SAML only)	contains metadata that specifies an access-domain attribute, the firewall automatically populates this field with that attribute. The firewall matches its locally configured access domains with those retrieved from SAML messages to enforce access control. If a SAML message has multiple access-domain values for an administrator with only one access domain, matching applies only to the first (left-most) value in the access-domain attribute. For an administrator with more than one access domain, the matching can apply to multiple values in the attribute.
Factors Tab	
Enable Additional Authentication Factors	Select this option if you want the firewall to invoke additional authentication factors (challenges) after users successfully respond to the first factor (specified in the **Type** field on the **Authentication** tab).  *Additional authentication factors are supported for end-user authentication through Authentication Policy only. Additional factors are not supported for remote user authentication to GlobalProtect portals and gateways or for administrator authentication to the PAN-OS or Panorama web interface. Although you can configure additional factors, they will not be enforced for these use cases. You can, however, integrate with MFA vendors using RADIUS or SAML for all authentication use cases.* After configuring an authentication profile that uses multi-factor authentication (MFA), you must assign it to an authentication enforcement object (Objects>Authentication) and assign the object to the Authentication policy rules (Policies>Authentication) that control access to your network resources.
Factors	Add an MFA server profile (Device>ServerProfiles> Multi Factor Authentication) for each authentication factor that the firewall will invoke after users successfully respond to the first factor (specified in the **Type** field on the **Authentication** tab). The firewall invokes each factor in the top-to-bottom order that you list the MFA services that provide the factors. To change the order, select a server profile and **Move Up** or **Move Down**. You can specify up to three additional factors. Each MFA service provides one factor. Some MFA services let users choose one factor from a list of several. The firewall integrates with these MFA services through vendor APIs. Additional MFA vendor API integrations are added periodically through Applications or Applications and Threats content updates.
Advanced Tab	
Allow List	Click **Add** and select **all** or select the specific users and groups that can authenticate with this profile. When a user authenticates, the firewall matches the associated username or group against the entries in this list. If you don't add entries, no users can authenticate.  *To limit authentication to only the users who have legitimate business access needs and reduce the attack surface, specify users or user groups, don't use all.*

Authentication Profile Settings	Description
	*If you entered a User Domain value, you don't need to specify domains in the Allow List. For example, if the User Domain is **businessinc** and you want to add user **admin1** to the Allow List, entering **admin1** has the same effect as entering **businessinc\admin1**. You can specify groups that already exist in your directory service or specify custom groups based on LDAP filters.*
Failed Attempts (All authentication types except SAML)	Enter the number of failed successive login attempts (0 to 10) that the firewall allows before locking out the user account. A value of 0 specifies unlimited login attempts. The default value is 0 for firewalls in normal operational mode and 10 for firewalls in FIPS-CC mode. *Set the number of Failed Attempts to 5 or fewer to accommodate a reasonable number of retries in case of typing errors, while preventing malicious systems from trying brute force methods to log in to the firewall.* *If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, the Failed Attempts is ignored and the user is never locked out.*
Lockout Time (All authentication types except SAML)	Enter the number of minutes (range is 0 to 60; default is 0) for which the firewall locks out a user account after the user reaches the number of **Failed Attempts**. A value of 0 means the lockout applies until an administrator manually unlocks the user account. *Set the Lockout Time to at least 30 minutes to prevent continuous login attempts from a malicious actor.* *If you set the Lockout Time to a value other than 0 but leave the Failed Attempts at 0, the Lockout Time is ignored and the user is never locked out.*

SAML Metadata Export from an Authentication Profile

- Device > Authentication Profile

The firewall and Panorama can use a SAML identity provider (IdP) to authenticate users who request services. For administrators, the service can be access to the web interface. For end users, the service can be Authentication Portal or GlobalProtect, which enable access to your network resources. To enable SAML authentication for a service, you must register that service by entering specific information about it on the IdP in the form of SAML metadata. The firewall and Panorama simplify registration by automatically generating a SAML metadata file based on the authentication profile that you assigned to the service and you can export this metadata file to the IdP. Exporting the metadata is an easier alternative to typing the values for each metadata field in the IdP.

Some of the metadata in the exported file derives from the SAML IdP server profile assigned to the authentication profile (Device > Server Profiles > SAML Identity Provider). However,

the exported file always specifies POST as the HTTP binding method, regardless of the method specified in the SAML IdP server profile. The IdP will use the POST method to send SAML messages to the firewall or Panorama.

To export SAML metadata from an authentication profile, click the SAML **Metadata** link in the Authentication column and complete the following fields. To import the metadata file into an IdP, refer to your IdP documentation.

SAML Metadata Export Settings	Description
Commands	Select the service for which you want to export SAML metadata: • **management** (default)—Provides administrator access to the web interface. • **authentication-portal**—Provides end user access to network resources through Authentication Portal. • **global-protect**—Provides end user access to network resources through GlobalProtect. Your selection determines which other fields the dialog displays.
[Management | Authentication Portal | GlobalProtect] Auth Profile	Enter the name of the authentication profile from which you are exporting metadata. The default value is the profile from which you opened the dialog by clicking the **Metadata** link.
Management Choice (Management only)	Select an option for specifying an interface that is enabled for management traffic (such as the MGT interface): • **Interface**—Select the interface from the list of interfaces on the firewall. • **IP Hostname**—Enter the IP address or hostname of the interface. If you enter a hostname, the DNS server must have an address (A) record that maps to the IP address.
[Authentication Portal | GlobalProtect] Virtual System (Authentication Portal or GlobalProtect only)	Select the virtual system for which the Authentication Portal settings or GlobalProtect portal are defined.
IP Hostname (Authentication Portal or GlobalProtect only)	Enter the IP address or hostname of the service. • **Authentication Portal**—Enter the **Redirect Host** IP address or hostname (**Device** > **User Identification** > **Authentication Portal Settings**). • **GlobalProtect**—Enter the **Hostname** or **IP Address** of the GlobalProtect portal. If you enter a hostname, the DNS server must have an address (A) record that maps to the IP address.

Device > Authentication Sequence

- Device > Authentication Sequence
- Panorama > Authentication Sequence

In some environments, user accounts reside in multiple directories (such as LDAP and RADIUS). An authentication sequence is a set of authentication profiles that the firewall tries to use for authenticating users when they log in. The firewall tries the profiles sequentially from the top of the list to the bottom—applying the authentication, Kerberos single sign-on, allow list, and account lockout values for each—until one profile successfully authenticates the user. The firewall only denies access if all profiles in the sequence fail to authenticate. For details on authentication profiles, see Device > Authentication Profile.

Configure an authentication sequence with multiple authentication profiles that use different authentication methods. Configure at least two external authentication methods and one local (internal) method so connectivity issues don't prevent authentication. Make the local authentication profile the last profile in the sequence so it's only used if all external authentication methods fail. (External authentication provides dedicated, reliable, centralized authentication services, including logging and troubleshooting features.)

Authentication Sequence Settings	Description
Name	Enter a name to identify the sequence. The name is case-sensitive, can have up to 31 characters, and can include only letters, numbers, spaces, hyphens, underscores, and periods. The name must be unique in the current **Location** (firewall or virtual system) relative to other authentication sequences and to authentication profiles. *In a firewall that has multiple virtual systems, if the Location of the authentication sequence is a virtual system (vsys), don't enter the same name as an authentication profile in the Shared location. Similarly, if the sequence Location is Shared, don't enter the same name as a profile in a vsys. While you can commit an authentication sequence and profile with the same names in these cases, reference errors might occur.*
Location	Select the scope in which the sequence is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the sequence, you can't change its **Location**.
Use domain to determine authentication profile	Select this option (selected by default) if you want the firewall to match the domain name that a user enters during login with the **User Domain** or **Kerberos Realm** of an authentication profile associated with the sequence and then use that profile to authenticate the user. The user input that the firewall uses for matching can be the text preceding the username (with a backslash separator) or the text following the username (with a @ separator). If the firewall does not find a match, it tries the authentication profiles in the sequence in top-to-bottom order.

Authentication Sequence Settings	Description
Authentication Profiles	Click **Add** and select from the drop-down for each authentication profile you want to add to the sequence. To change the list order, select a profile and click **Move Up** or **Move Down**. To remove a profile, select it and click **Delete**.  *You cannot add an authentication profile that specifies a multi-factor authentication (MFA) server profile or a Security Assertion Markup Language (SAML) Identity Provider server profile.*

Device > Data Redistribution

These settings define the methods that the firewall or Panorama uses to redistribute data.

What are you looking for?	See:
Add or delete data redistribution agents.	Device > Data Redistribution > Agents
View information on data redistribution clients.	Device > Data Redistribution > Clients
Configure the data redistribution agent collector name and pre-shared key.	Device > Data Redistribution > Collector Settings
Define the subnetworks that the data redistribution agent includes or excludes when redistributing data.	Device > Data Redistribution > Include/Exclude Networks

Device > Data Redistribution > Agents

Add a data redistribution agent using a serial number or host and port information.

Data Redistribution Agent Settings	Description
Name	Enter a name for the data redistribution agent (up to 31 characters). Use only letters, numbers, spaces, hyphens, and underscores.
Enabled	Select this option to enable the data redistribution agent.
Add an Agent Using	Select how you want to add the data redistribution agent: • **Serial Number**— Select this option and then select the Serial Number. • **Host and Port**—Select this option and enter the following host and port information: • **Host**—Enter the hostname. • **LDAP Proxy**—Select this option to use the host as an LDAP proxy. • **Port**—Enter the port number where the agent listens for requests. • **Collector Name**—Enter the **Collector Name** and **Pre-Shared Key** that identify the firewall or virtual system as a User-ID agent.
Data type	Select the type of data that you want to redistribute (IP User Mappings, IP Tags, User Tags, HIP, or Quarantine List).

After you configure a data redistribution agent, you can view the following information for the redistribution agent:

Data Redistribution Agent Information	Description
Serial Number	The identification number of the agent.
Host	The information for the host.
Collector Name	The name of the collector agent.
HIP	The host information profile of the agent.
IP User Mappings	The IP address-to-username mapping information.
IP Tags	The IP address-to-tag mapping information.
Quarantine List	Displays a list of devices that are in quarantine.
Dynamic User Group	The username-to-tag mapping information.
Connected	Indicates if the agent is connected to the redistribution service.

Device > Data Redistribution > Clients

Select **Device** > **Data Redistribution** > **Clients** to display the following information for each redistribution client:

Redistribution Agent Information	Description
Host information	The host information for the client.
Port	The port the redistribution client uses.
Vsys ID	The identification for the virtual system to which the redistribution client is connected.
Version	The PAN-OS version of the client.
Status	Displays the status of the redistribution client.
PDF/CSV	Administrative roles with a minimum of read-only access can export the data redistribution information as **PDF/CSV**.
Refresh Connected	Updates the information for all connected redistribution clients.

Device > Data Redistribution > Collector Settings

To configure a connection to a User-ID redistribution agent, enter a name for the collector and the pre-shared key.

Data Redistribution Agent Setup Settings	Description
Collector Name	Enter a **Collector Name** (up to 255 alphanumeric characters) to identify the redistribution agent.
Collector Pre-Shared Key / Confirm Collector Pre-Shared Key	Enter and confirm the **Pre-Shared Key** (up to 255 alphanumeric characters) for the collector.

Device > Data Redistribution > Include/Exclude Networks

Use the Include/Exclude Networks list to define the subnetworks that the redistribution agent includes or excludes when it redistributes the mappings.

Task	Description
Add	To limit discovery to a specific subnetwork, **Add** a subnetwork profile and complete the following fields: • **Name**—Enter a name to identify the subnetwork. • **Enabled**—Select this option to enable inclusion or exclusion of the subnetwork for server monitoring. • **Discovery**—Select whether the User-ID agent will **Include** or **Exclude** the subnetwork. • **Network Address**—Enter the IP address range of the subnetwork. The agent applies an implicit exclude all rule to the list. For example, if you add subnetwork 10.0.0.0/8 with the **Include** option, the agent excludes all other subnetworks even if you don't add them to the list. Add entries with the **Exclude** option only if you want the agent to exclude a subset of the subnetworks you explicitly included. For example, if you add 10.0.0.0/8 with the **Include** option and add 10.2.50.0/22 with the **Exclude** option, the User-ID agent will perform discovery on all the subnetworks of 10.0.0.0/8 except 10.2.50.0/22, and will exclude all subnetworks outside of 10.0.0.0/8. If you add **Exclude** profiles without adding any **Include** profiles, the agent excludes all subnetworks, not just the ones you added.
Delete	To remove a subnetwork from the list, select and **Delete** it. **Tip**: To remove a subnetwork from the Include/Exclude Networks list without deleting its configuration, edit the subnetwork profile and clear **Enabled**.
Custom Include/ Exclude Network	By default, the agent evaluates the subnetworks in the order you add them, from top-first to bottom-last. To change the evaluation order, click **Custom Include/ Exclude Network Sequence**. You can then **Add**, **Delete**, **Move Up**, or **Move Down** the subnetworks to create a custom evaluation order.

Device > Device Quarantine

The **Device** > **Device Quarantine** page displays the devices that are in the quarantine list. A device appears in this list as a result of the following actions:

- The system administrator added the device to this list manually.

  To manually **Add** a device, enter the **Host ID** and, optionally, the **Serial Number** of the device you need to quarantine.
- The system administrator selected the Host ID column from the Traffic, GlobalProtect, or Threat log, selected a device from that column, and then selected **Block Device**.
- The device matched a Security policy rule that has a log forwarding profile whose match list had a built-in action set to **Quarantine**.

  The Host ID displays in the GlobalProtect logs automatically. For the Host ID to display in the Traffic, Threat, or Unified logs, the firewall must have at least one security policy rule with the Source Device set to Quarantine. Without this setting in the security policy, Traffic, Threat or Unified logs will not have the Host ID, and the log forwarding profile will not take effect.
- The device was added to the quarantine list using an API.
- The firewall received the quarantine list as a part of redistributed entry (the quarantine list was redistributed from another Panorama appliance or firewall).

The Device Quarantine table includes the following fields.

Field	Description
Host ID	The Host-ID of the host that is blocked.
Reason	The reason that the device is quarantined. A reason of **Admin Add** means that an administrator manually added the device to the table.
Time Stamp	The time that the administrator or Security policy rule added the device to the quarantine list.
Source Device/App	The IP address of the Panorama, firewall, or third-party app that added the device to the quarantine list.
Serial Number	(Optional) The serial number of the quarantined device (if available).
User Name	(Optional) The username of the GlobalProtect client user who was logged in to the device when it was quarantined.

Device > VM Information Sources

Use this tab to proactively track changes on the Virtual Machines (VMs) deployed on any of these sources—VMware ESXi server, VMware vCenter server, Amazon Web Services Virtual Private Cloud (AWS-VPC), or Google Compute Engine (GCE).

When monitoring ESXi hosts that are part of the VM-Series NSX edition solution, use Dynamic Address Groups instead of using VM Information Sources to learn about changes in the virtual environment. For the VM-Series NSX edition solution, the NSX Manager provides Panorama with information on the NSX security group to which an IP address belongs. The information from the NSX Manager provides the full context for defining the match criteria in a Dynamic Address Group because it uses the service profile ID as a distinguishing attribute and allows you to properly enforce policy when you have overlapping IP addresses across different NSX security groups.

You can register up to a maximum of 32 tags to an IP address.

There are two ways to monitor VM Information Sources:

- The firewall can monitor your VMware ESXi server, VMware vCenter server, GCE instances, or AWS-VPCs, and retrieve changes as you provision or modify the guests configured on the monitored sources. For each firewall or for each virtual system on a firewall configured with multiple virtual systems, you can configure up to 10 sources.

  The following conditions apply when your firewalls are configured in a high availability (HA) configuration:

  - **Active/passive HA configuration**—Only the active firewall monitors the VM information sources.
  - **Active/active HA configuration**—Only the firewall with the `primary` priority value monitors the VM information sources.

  For information on how VM Information Sources and Dynamic Address Groups can work synchronously and enable you to monitor changes in the virtual environment, refer to the VM-Series Deployment Guide.
- For IP address-to-username mapping, you can configure the VM Information Sources on either the Windows User-ID agent or on the firewall to monitor the VMware ESXi and vCenter server and retrieve changes as you provision or modify the guests configured on the server. The Windows User-ID agent supports up to 100 sources. Support for AWS and Google Compute Engine is not available for the User-ID agent.

  Each VM on a monitored ESXi or vCenter server must have VMware Tools installed and running. VMware Tools provide the ability to IP address and other values assigned to each VM.

To collect the values assigned to the monitored VMs, the firewall monitors the attributes in the following tables.

Attributes Monitored on a VMware Source

- UUID
- Name
- Guest OS
- Annotation
- VM State — the power state can be `poweredOff`, `poweredOn`, `standBy`, or `unknown`.

Attributes Monitored on a VMware Source
• Version • Network—Virtual Switch Name, Port Group Name, and VLAN ID • Container Name—vCenter Name, Data Center Object Name, Resource Pool Name, Cluster Name, Host, and Host IP address.

Attributes Monitored on the AWS-VPC
• Architecture • Guest OS • Image ID • Instance ID • Instance State • Instance Type • Key Name • Placement—Tenancy, Group Name, and Availability Zone • Private DNS Name • Public DNS Name • Subnet ID • Tag (key, value); up to 18 tags supported per instance • VPC ID

Attributes Monitored for Google Compute Engine (GCE)
• Hostname of the VM • Machine type • Project ID • Source (OS type) • Status • Subnetwork • VPC Network • Zone

Add—**Add** a new source for VM Monitoring and fill in the details based on the source you are monitoring:

- For VMware ESXi or vCenter Server, see Settings to Enable VM Information Sources for VMware ESXi and vCenter Servers.
- For AWS-VPC, see Settings to Enable VM Information Sources for AWS VPC.
- For Google Compute Engine (GCE), see Settings to Enable VM Information Sources for Google Compute Engine.

Refresh Connected—Refreshes the connection status in the on-screen display; this does not refresh the connection between the firewall and the monitored sources.

Delete—Deletes any configured VM Information source that you select.

PDF/CSV—Exports the VM Information source configuration table as a PDF or comma-separated values (CSV) file. See Configuration Table Export.

Settings to Enable VM Information Sources for VMware ESXi and vCenter Servers

The following table describes settings you can configure to enable VM information sources for VMware ESXi and vCenter servers.

To retrieve the tags for the virtual machines, the firewall requires an account with read-only access on the VMware ESXi and vCenter servers.

Settings to Enable VM Information Sources for VMware ESXi or vCenter Server	
Name	Enter a name to identify the monitored source (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Type	Select whether the host/source being monitored is an **ESXi server** or **vCenter server**.
Description	(Optional) Add a label to identify the location or function of the source.
Port	Specify the port on which the host/source is listening. (default port 443).
Enabled	By default the communication between the firewall and the configured source is enabled. The connection status between the monitored source and the firewall displays in the interface as follows: • Connected • Disconnected • Pending; the connection status also displays as yellow when the monitored source is disabled. Clear the **Enabled** option to disable communication between the host and the firewall.
Timeout	Enter the interval in hours after which the connection to the monitored source is closed, if the host does not respond (range is 2–10; default is 2). (Optional) To change the default value, **Enable timeout when the source is disconnected** and specify a value. When the specified limit is reached, if the host is inaccessible, or if the host does not respond, the firewall will close the connection to the source.
Source	Enter the FQDN or the IP address of the host/source being monitored.
Username	Specify the username required to authenticate to the source.
Password	Enter the password and confirm your entry.
Update Interval	Specify the interval, in seconds, at which the firewall retrieves information from the source (range is 5–600; default is 5).

Settings to Enable VM Information Sources for AWS VPC

The following table describes the setting you configure to enable VM information sources for an AWS VPC.

Settings to Enable VM Information Sources for AWS VPC	
Name	Enter a name to identify the monitored source (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Type	Select **AWS VPC**.
Description	(Optional) Add a label to identify the location or function of the source.
Enabled	By default the communication between the firewall and the configured source is enabled. The connection status between the monitored source and the firewall displays in the interface as follows: • Connected • Disconnected • Pending; The connection status also displays as yellow when the monitored source is disabled. Clear the **Enabled** option to disable communication between the host and the firewall.
Source	Add the URI in which the Virtual Private Cloud resides. For example, ec2.us-west-1.amazonaws.com The syntax is: ec2.<*your_AWS_region*>.amazonaws.com; for AWS China it is: ec2.<AWS_region>.amazonaws.com.cn
Access Key ID	Enter the alphanumeric text string that uniquely identifies the user who owns or is authorized to access the AWS account. This information is a part of the AWS Security Credentials. The firewall requires the credentials—Access Key ID and the Secret Access Key—to digitally sign API calls made to the AWS services.
Secret Access Key	Enter the password and confirm your entry.
Update Interval	Specify the interval, in seconds, at which the firewall retrieves information from the source (range is 60 to 1,200; default is 60).
Timeout	The interval in hours after which the connection to the monitored source is closed, if the host does not respond (default is 2) (Optional) **Enable timeout when the source is disconnected**. When the specified limit is reached, if the source is inaccessible, or if the source does not respond, the firewall will close the connection to the source.
VPC ID	Enter the ID of the AWS-VPC to monitor, for example, vpc-1a2b3c4d. Only EC2 instances that are deployed within this VPC are monitored.

Settings to Enable VM Information Sources for AWS VPC	
	If your account is configured to use a default VPC, the default VPC ID will be listed under AWS Account Attributes.

Settings to Enable VM Information Sources for Google Compute Engine

Device > **VM Information Sources** > **Add**

The following table describes the settings you need to configure to enable VM Information Sources for Google Compute Engine instances on Google Cloud Platform. Enable monitoring of Google Compute Engine (GCE) instances to allow the firewall (physical or virtual on-premise, or running in Google Cloud) to retrieve tag, label, and other metadata about the instances running in a particular Google Cloud zone of the specified project. For information on the VM-Series on Google Cloud Platform, refer to the VM-Series Deployment Guide.

Settings to Enable VM Information Sources for Google Compute Engine	
Name	Enter a name to identify the monitored source (up to 31 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores.
Type	Select **Google Compute Engine**.
Description	(Optional) Add a label to identify the location or function of the source.
Enabled	The communication between the firewall and the configured source is enabled by default. The connection status between the monitored source and the firewall displays in the interface as follows: • —Connected • —Disconnected • —Pending or the monitored source is disabled. Clear the **Enabled** option to disable communication between the configured source and the firewall. When you disable communication, all the registered IP address and tags are removed from the associated dynamic address group. This means that policy rules will not apply to the GCE instances from this Google Cloud Project.
Service Authentication Type	Select VM-Series running on GCE or Service Account. • **VM-Series running on GCE**—Select this option if the hardware-based or VM-Series firewall on which you are enabling VM Monitoring is not deployed within the Google Cloud Platform. • **Service Account**—Select this option if you are monitoring Google Cloud Engine instances on a firewall that is not deployed on the Google Cloud Platform. This option allows you to use a special

Settings to Enable VM Information Sources for Google Compute Engine	
	Google account that belongs to the virtual machine or application instead of using an individual end-user account. The service account must have the IAM policies (**Compute Engine** > **Compute Viewer** privilege) that authorize access to the Google API and that allow it to query the virtual machines in the Google Cloud Project for virtual machine metadata.
Service Account Credential	(Only for Service Account) Upload the JSON file with the credentials for the service account. This file allows the firewall to authenticate to the instance and authorizes access to the metadata. You can create an account on the Google Cloud console (**IAM & admin** > **Service Accounts**). Refer to the Google documentation for information on how to create an account, add a key to it, and download the JSON file that you need to upload to the firewall.
Project ID	Enter the alphanumeric text string that uniquely identifies the Google Cloud Project that you want to monitor.
Zone Name	Enter the zone information as a string of up to 63 characters in length. For example: **`us-west1-a`**.
Update Interval	Specify the interval (in seconds) at which the firewall retrieves information from the source (range is 60 to 1,200; default is 60).
Timeout	The interval (in hours) after which the connection to the monitored source is closed if the host does not respond (default is 2). (Optional) **Enable timeout when the source is disconnected**. When the specified limit is reached, if the source is inaccessible or does not respond, the firewall will close the connection to the source. When the source is disconnected, all the IP addresses and tags that were registered from this project are removed from the dynamic address group.

Device > Troubleshooting

- **Device** > **Troubleshooting**
- **Panorama** > **Managed Devices** > **Troubleshooting**

Before committing device group or template configuration changes, test the functionality from the web interface to verify that the changes did not introduce connectivity issues are introduced in the running configuration and that your policies correctly allow or deny traffic.

- **Policy Match Tests**
  - Security Policy Match
  - QoS Policy Match
  - Authentication Policy Match
  - Decryption/SSL Policy Match
  - NAT Policy Match
  - Policy Based Forwarding Policy Match
  - DoS Policy Match
- **Connectivity Tests**
  - Routing
  - Test Wildfire
  - Threat Vault
  - Ping
  - Trace Route
  - Log Collector Connectivity
  - External Dynamic List
  - Update Server
  - Test Cloud Logging Service Status
  - Test Cloud GP Service Status

Security Policy Match

Field	Description
Test Configuration	
Select Test	Select the policy match test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
From	Enter the zone where the traffic originated.
To	Select the destination zone of the traffic.

Field	Description
Source	Enter the IP address where the traffic originated.
Destination	Enter the destination IP address of the traffic.
Destination Port	Enter the specific destination port for which traffic is intended.
Source User	Enter the user from which the traffic originated.
Protocol	Enter the IP protocol used for routing. Can be 0 to 255.
Show all potential match rules until first allow rule	Enable this option to show all potential rule matches until the first matched rule result. Disable (clear) to return only the first matched rule in the test results.
Application	Select the application traffic you want to test.
Category	Select the traffic category you want to test.
(Firewall only) Check HIP mask	Select to check the security status of the end device that is accessing your network.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped. • `Shared policy disabled on device`—The Panorama settings on the device do not allow for the policy to be pushed from Panorama.

QoS Policy Match

Field	Description
Test Configuration	
Select Test	Select the policy match test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group &

Field	Description
	Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
From	Enter the zone where the traffic originated.
To	Select the destination zone of the traffic.
Source	Enter the IP address where the traffic originated.
Destination	Enter the destination IP address of the traffic.
Destination Port	Enter the specific destination port for which traffic is intended.
Source User	Select the user from which the traffic originated.
Protocol	Enter the IP protocol used for routing. Can be 0 to 255.
Application	Select the application traffic you want to test.
Category	Select the traffic category you want to test.
Codepoint Type	Select the type of codepoint encoding you want to test.
Codepoint Value	Specify the value of the codepoint encoding: • **DSCP**—0 to 63 • **ToS**—0 to 7
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped. • `Shared policy disabled on device`—The Panorama settings on the device do not allow for the policy to be pushed from Panorama.

Authentication Policy Match

Field	Description
Test Configuration	
Select Test	Select the policy match test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
From	Enter the zone where the traffic originated.
To	Select the destination zone of the traffic.
Source	Enter the IP address where the traffic originated.
Destination	Enter the destination IP address of the traffic.
Category	Select the traffic category you want to test.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped. • `Shared policy disabled on device`—The Panorama settings on the device do not allow for the policy to be pushed from Panorama.

Decryption/SSL Policy Match

Field	Description
Test Configuration	

Field	Description
Select Test	Select the policy match test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
From	Enter the zone where the traffic originated.
To	Select the destination zone of the traffic.
Source	Enter the IP address where the traffic originated.
Destination	Enter the destination IP address of the traffic.
Application	Select the application traffic you want to test.
Category	Select the traffic category you want to test.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

NAT Policy Match

Field	Description
Test Configuration	
Select Test	Select the policy match test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems

Field	Description
	based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
From	Enter the zone where the traffic originated.
To	Select the destination zone of the traffic.
Source	Enter the IP address where the traffic originated.
Destination	Enter the destination IP address of the traffic.
Source Port	Enter the specific port the traffic originated from.
Destination Port	Enter the specific destination port for which traffic is intended.
Protocol	Enter the IP protocol used for routing. Can be 0 to 255.
To Interface	Enter the destination interface on the device for which the traffic is intended.
HA Device ID	Enter the ID of the HA device: • **0**—Primary HA peer • **1**—Secondary HA peer
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped. • `Shared policy disabled on device`—The Panorama settings on the device do not allow for the policy to be pushed from Panorama.

Policy Based Forwarding Policy Match

Field	Description
Test Configuration	
Select Test	Select the policy match test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
From	Enter the zone where the traffic originated.
From Interface	Enter the interface on the device from which the traffic originated.
Source	Enter the IP address where the traffic originated.
Destination	Enter the destination IP address of the traffic.
Destination Port	Enter the specific destination port for which traffic is intended.
Source User	Enter the user from which the traffic originated.
Protocol	Enter the IP protocol used for routing. Can be 0 to 255.
Application	Select the application traffic you want to test.
HA Device ID	ID of the HA device: • **0**—Primary HA peer • **1**—Secondary HA peer
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

Field	Description
	• `Shared policy disabled on device`—The Panorama settings on the device do not allow for the policy to be pushed from Panorama.

DoS Policy Match

Field	Description
Test Configuration	
Select Test	Select the policy match test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
From	Enter the zone where the traffic originated.
To	Select the destination zone of the traffic.
From Interface	Enter the interface on the device from which the traffic originated.
To Interface	Enter the destination interface on the device for which the traffic is intended.
Source	Enter the IP address where the traffic originated.
Destination	Enter the destination IP address of the traffic.
Destination Port	Enter the specific destination port for which traffic is intended.
Source User	Enter the user from which the traffic originated.
Protocol	Enter the IP protocol used for routing. Can be 0 to 255.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`.

Field	Description
	• Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

Routing

Field	Description
Select Test	Select the connectivity test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
FiB Lookup, Mfib Lookup	Select one of the following for Lookup: • **FiB**—Perform route lookup within activate route table • **Mfib**—Perform multicast route lookup within active route table
Destination IP	Enter the IP address for which the traffic is intended .
Virtual Router	Specific virtual router within which the routing test is performed. Select the virtual router from the drop-down.
ECMP	
Source IP	Enter the specific IP address from which the traffic originated.
Source Port	Enter the specific port from which the traffic originated.
Destination IP	Enter the specific IP address for which the traffic is intended.
Destination Port	Enter the specific destination port for which the traffic is intended.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`.

Field	Description
	• Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

Test Wildfire

Field	Description
Select Test	Select the connectivity test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
Channel	Select the Wildfire channel: **`Public`** or **`Private`**.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

Threat Vault

Field	Description
Select Test	Select the connectivity test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems

Field	Description
	based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

Ping

The ping troubleshooting test is only supported on firewalls running PAN-OS 9.0 or later releases.

Field	Description
Select Test	Select the connectivity test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
Bypass routing table, use specified interface	Enable this option to bypass the routing table and use a specified interface. Disable (clear) this option to test the configured routing table.
Count	Enter the number of requests to send. The default count is 5.
Don't fragment echo request packets (IPv4)	Enable this option to not fragment the echo request packets for the test. Disable
Force to IPv6 destination	Enable to force test to the IPv6 destination.

Field	Description
Interval	Specify a delay, in seconds, between requests (range is 1 to 2,000,000,000).
Source	Enter the source address of the echo request.
Don't attempt to print addresses symbolically	Enable this option to display IP addresses in test results and not resolve the IP address hostname. Disable (clear) to resolve IP address hostnames.
Pattern	Specify the hexadecimal fill pattern.
Size	Enter the size, in bytes, of the request packets (range is 0 to 65468).
ToS	Enter the IP type-of-service value (range is 1 to 255).
TTL	Enter the IP time-to-live value in hops—IPv6 hop-limit value (range is 1 to 255).
Display detailed output	Enable to display a detailed output of the test results.
Host	Enter the hostname or IP address of the remote host.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

Trace Route

Field	Description
Select Test	Select the connectivity test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.

Field	Description
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
Use IPv4	Enable to use the IPv4 address of the selected devices.
Use IPv6	Enable to use the IPv6 address of the selected devices.
First TTL	Enter the time-to-live used in the first outgoing probe packet (range is 1 to 255).
Max TTL	Enter the maximum time-to-live hops (range is 1 to 255).
Port	Enter the base port number used in probe.
ToS	Enter the IP type-of-service value (range is 1 to 255).
Wait	Enter the number of seconds to wait for a response (range is 1 to 99,999).
Pause	Enter the time, in milliseconds, to pause between probes (range is 1 to 2,000,000,000).
Set the “don’t fragment” bit	Enable this option to not fragment the ICMP packet in to multiple packets if the path cannot support the configured maximum transmission unit (MTU).
Enable socket level debugging	Enable this option to allows you to debug on the socket level.
Gateway	Specify a maximum of 8 loose source route gateways.
Don’t attempt to print addresses symbolically	Enable this option to display IP addresses in test results and not resolve the IP address hostname. Disable (clear) to resolve IP address hostnames.
Bypass routing tables and send directly to a host	Enable this option to bypass any configured routing tables and test directly with the host.
Source	Enter a source address in outgoing probe packets.
Host	Enter the hostname or IP address of the remote host.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`.

Field	Description
	• Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

Log Collector Connectivity

Field	Description
Select Test	Select the connectivity test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems that have been selected for testing.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

External Dynamic List

Field	Description
Select Test	Select the connectivity test to execute.
(Panorama only) Select device	**Select device/VSYS** to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.

Field	Description
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
URL Test	Specify the URL for testing the connection.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

Update Server

Field	Description
Select Test	Select the connectivity test to execute.
Results	Select to view the Result Details of the executed test. (Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed: • `N/A`—Test was not applicable to the device. • `Device not connected`—Device connection was dropped.

Test Cloud Logging Service Status

Test the connectivity status to the Cloud Logging Service. This test is only available on a Panorama management server running the Cloud Services plugin version 1.3 or later installed.

Field	Description
Select Test	Select the connectivity test to execute.
Results	Select to view the Result Details of the executed test. When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed:

Test Cloud GP Service Status

Test the connectivity status to GlobalProtect as a Service. This test is only available on a Panorama management server running the Cloud Services plugin version 1.3 or later installed.

Field	Description
Select Test	Select the connectivity test to execute.
Results	Select to view the Result Details of the executed test. When executing the test for multiple managed devices, the Results display the following information for each device tested: • Device Group—Name of the device group to which the firewall that is processing traffic belongs. • Firewall—Name of the firewall that is processing traffic • Status—Indicates the status of the test: `Success` or `Failure`. • Result—Displays the test result. If the test could not be performed, one of the following is displayed:

Device > Virtual Systems

A virtual system (vsys) is an independent (virtual) firewall instance that you can separately manage within a physical firewall. Each vsys can be an independent firewall with its own Security policy, interfaces, and administrators; a vsys enables you to segment the administration of all policies, reporting, and visibility functions that the firewall provides.

For example, if you want to customize the security features for the traffic that is associated with your Finance department, you can define a Finance vsys and then define security policies that pertain only to that department. To optimize policy administration, you can maintain separate administrator accounts for overall firewall and network functions while creating vsys administrator accounts that allow access to an individual vsys. This allows the vsys administrator in the Finance department to manage the Security policy for only that department.

Networking functions (such as static and dynamic routing, IP addresses of interfaces, and IPSec tunnels) pertain to an entire firewall and all of its virtual systems. A virtual system configuration (**Device** > **Virtual Systems**) doesn't control firewall-level and network-level functions (such as static and dynamic routing, IP addresses of interfaces, IPSec tunnels, VLANs, virtual wires, virtual routers, GRE tunnels, DHCP, DNS Proxy, QoS, LLDP and network profiles). For each vsys, you can specify a collection of physical and logical firewall interfaces (including VLANs and virtual wires) and security zones. If you require routing segmentation for each vsys, you must create and assign additional virtual routers and assign interfaces, VLANs, and virtual wires as needed.

If you use a Panorama template to define your virtual systems, you can configure one vsys to be the default. The default vsys and Multi Virtual System Capability determine whether a firewall accepts vsys-specific configurations during a template commit:

- Firewalls that have Multi Virtual System Capability enabled accept vsys-specific configurations for any vsys that is defined in the template.
- Firewalls that don't have Multi Virtual System Capability enabled accept vsys-specific configurations only for the default vsys. If you do not configure a default vsys, then these firewalls will not accept vsys-specific configurations.

PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls support multiple virtual systems. However, PA-3200 Series firewalls require a license for enabling multiple virtual systems. The PA-220 and PA-800 Series firewalls do not support multiple virtual systems.

Before enabling multiple virtual systems, consider the following:

- A vsys administrator creates and manages all items needed for Security policy per assigned virtual system.
- Zones are objects within a vsys. Before defining a policy or policy object, select the appropriate **Virtual System** from the drop-down on the **Policies** or **Objects** tab.
- You can set remote logging destinations (SNMP, syslog, and email), applications, services, and profiles to be available to all virtual systems (shared) or to a single vsys.
- If you have multiple virtual systems, you can select a vsys as a User-ID hub to share the IP address-to-username mapping information between virtual systems.
- You can configure globally (to all virtual systems on a firewall) or vsys-specific service routes (Device > Setup > Services).
- You can rename a vsys only on the local firewall. On Panorama, renaming a vsys is not supported. If you rename a vsys on Panorama, the result is an entirely new vsys or the new vsys name gets mapped to the wrong vsys on the firewall.

Before defining a vsys, you must first enable the multi-vsys functionality on the firewall. Select **Device** > **Setup** > **Management**, edit the **General Settings**, select **Multi Virtual System Capability**, and click **OK**. This adds a **Device** > **Virtual Systems** page. Select the page, **Add** a vsys, and specify the following information.

Virtual System Settings	Description
ID	Enter an integer identifier for the vsys. Refer to the data sheet for your firewall model for information on the number of supported virtual systems. *If you use a Panorama template to configure the vsys, this field does not appear.*
Name	Enter a name (up to 31 characters) to identify the vsys. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. *If you use a Panorama template to push vsys configurations, the vsys name in the template must match the vsys name on the firewall.*
Allow Forwarding of Decrypted Content	Select this option to allow the virtual system to forward decrypted content to an outside service when port mirroring or sending WildFire files for analysis. See also Decryption Port Mirroring.
General Tab	Select a **DNS Proxy** object if you want to apply DNS proxy rules to this vsys. (Network > DNS Proxy). To include objects of a particular type, select that type (interface, VLAN, virtual wire, virtual router, or visible virtual system), **Add** an object, and select the object from the drop-down. You can add one or more objects of any type. To remove an object, select and **Delete** it.
Resource Tab	Specify the following resource limits allowed for this vsys. Each field displays the valid range of values, which varies per firewall model. The default setting is 0, which means the limit for the vsys is the limit for the firewall model. However, the limit for a specific setting isn't replicated for each vsys. For example, if a firewall has four virtual systems, each virtual system can't have the total number of Decryption Rules allowed per firewall. After the total number of Decryption Rules for all of the virtual systems reaches the firewall limit, you cannot add more. • **Sessions Limit**—Maximum number of sessions. *If you use the `show session meter` CLI command, the firewall displays the Maximum number of sessions allowed per dataplane, the Current number of sessions being used by the virtual system, and the Throttled number of sessions per virtual system. On PA-5200 Series and PA-7000 Series firewalls, the Current number of sessions being used can be greater than the Maximum configured for Sessions Limit because there are multiple dataplanes per virtual system. The Sessions Limit you configure on a PA-5200 Series or PA-7000 Series firewall is per dataplane and results in a higher maximum per virtual system.* • **Security Rules**—Maximum number of Security rules. • **NAT Rules**—Maximum number of NAT rules. • **Decryption Rules**—Maximum number decryption rules.

Virtual System Settings	Description
	• **QoS Rules**—Maximum number of QoS rules. • **Application Override Rules**—Maximum number of application override rules. • **Policy Based Forwarding Rules**—Maximum number of policy-based forwarding (PBF) rules. • **DoS Protection Rules**—Maximum number of denial-of-service (DoS) rules. • **Site to Site VPN Tunnels**—Maximum number of site-to-site VPN tunnels. • **Concurrent GlobalProtect Tunnels**—Maximum number of concurrent remote GlobalProtect users. • **Inter-Vsys User-ID Data Sharing**—**Make this vsys a User-ID data hub** to allow all other virtual systems on the firewall to access shared user mapping information or **Change hub** and select a new vsys to reassign that vsys as a User-ID data hub. Requires superuser or administrator privileges.

Device > Shared Gateways

Shared gateways allow multiple virtual systems to share a single interface for external communication (typically connected to a common upstream network such as an Internet Service Provider). All of the virtual systems communicate with the outside world through the physical interface using a single IP address. A single virtual router is used to route traffic for all of the virtual systems through the shared gateway.

Shared gateways use Layer 3 interfaces, and at least one Layer 3 interface must be configured as a shared gateway. Communications originating in a virtual system and exiting the firewall through a shared gateway require similar policy to communications passing between two virtual systems. You could configure an 'External vsys' zone to define security rules in the virtual system.

Shared Gateway Settings	Description
ID	Identifier for the gateway (not used by firewall).
Name	Enter a name for the shared gateway (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. Only the name is required.
DNS Proxy	(Optional) If a DNS proxy is configured, select which DNS server(s) to use for domain name queries.
Interfaces	Select the interfaces the shared gateway will use.

Device > Certificate Management

Device > Certificate Management > Certificates

Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** to manage (generate, import, renew, delete, and revoke) certificates, which are used to secure communication across a network. You can also export and import the high availability (HA) key that secures the connection between HA peers on the network. Select **Device** > **Certificate Management** > **Certificates** > **Default Trusted Certificate Authorities** to view, enable, and disable the certificate authorities (CAs) that the firewall trusts.

For more information on how to implement certificates on the firewall and Panorama, refer to Certificate Management.

- Manage Firewall and Panorama Certificates
- Manage Default Trusted Certificate Authorities
- Device > Certificate Management > Certificate Profile
- Device > Certificate Management > OCSP Responder
- Device > Certificate Management > SSL/TLS Service Profile
- Device > Certificate Management > SCEP
- Device > Master Key and Diagnostics

Manage Firewall and Panorama Certificates

- Device > Certificate Management > Certificates > Device Certificates
- Panorama > Certificate Management > Certificates

Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** or **Panorama** > **Certificate Management** > **Certificates** > **Device Certificates** to display the certificates that the firewall or Panorama uses for tasks such as securing access to the web interface, SSL decryption, or LSVPN.

The following are some uses for certificates. Define the usage of the certificate after you generate it (see Manage Default Trusted Certificate Authorities).

- **Forward Trust**—The firewall uses this certificate to sign a copy of the server certificate that the firewall presents to clients during SSL Forward Proxy decryption when the certificate authority (CA) that signed the server certificate is in the trusted CA list on the firewall.
- **Forward Untrust**—The firewall uses this certificate to sign a copy of the server certificate the firewall presents to clients during SSL Forward Proxy decryption when the CA that signed the server certificate is not in the trusted CA list on the firewall.
- **Trusted Root CA**—The firewall uses this certificate as a trusted CA for SSL Forward Proxy decryption, GlobalProtect, URL Admin Override, and Authentication Portal. The firewall has a large list of existing trusted CAs. The trusted root CA certificate is for additional CAs that your organization trusts but that are not part of the pre-installed trusted list.
- **SSL Exclude**—The firewall uses this certificate if you configure decryption exceptions to exclude specific servers from SSL/TLS decryption.
- **Certificate for Secure Syslog**—The firewall uses this certificate to secure the delivery of logs as syslog messages to a syslog server.

To generate a certificate, click Generate and specify the following fields:

After a certificate is generated, the page displays Other Supported Actions to Manage Certificates.

Settings to Generate a Certificate	Description
Certificate Type	Select the entity that generates the certificate: **Local**—The firewall or Panorama generates the certificate. **SCEP**—A Simple Certificate Enrollment Protocol (SCEP) server generates the certificate and sends it to the firewall or Panorama.
Certificate Name	(Required) Enter a name (up to 63 characters on the firewall or up to 31 characters on Panorama) to identify the certificate. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
SCEP Profile	(SCEP certificates only) Select a **SCEP Profile** to define how the firewall or Panorama communicates with a SCEP server and to define settings for the SCEP certificate. For details, see Device > Certificate Management > SCEP. You can configure a firewall that serves as a GlobalProtect portal to request SCEP certificates on demand and automaticallydeploy the certificates to endpoints. The remaining fields in the Generate Certificate dialog do not apply to SCEP certificates. After specifying the **Certificate Name** and **SCEP Profile**, click **Generate**.
Common Name	(Required) Enter the IP address or FQDN that will appear on the certificate.
Shared	On a firewall that has more than one virtual system (vsys), select **Shared** if you want the certificate to be available to every vsys.
Signed By	To sign the certificate, you can use a certificate authority (CA) certificate that you imported into the firewall. The certificate can also be self-signed, in which case the firewall is the CA. If you are using Panorama, you also have the option of generating a self-signed certificate for Panorama. If you imported CA certificates or issued any on the firewall (self-signed), the drop-down includes the CAs available to sign the certificate that you are creating. To generate a certificate signing request (CSR), select **External Authority (CSR)**. After the firewall generates the certificate and the key pair, you can export the CSR and send it to the CA for signing.
Certificate Authority	Select this option if you want the firewall to issue the certificate. Marking this certificate as a CA allows you to use this certificate to sign other certificates on the firewall.
Block Private Key Export	When you generate a certificate, select this option to block all administrators, including Superusers, from exporting the private key.
OCSP Responder	Select an OCSP responder profile from the drop-down (see Device > Certificate Management > OCSP Responder). The corresponding host name appears in the certificate.

Settings to Generate a Certificate	Description
Algorithm	Select a key generation algorithm for the certificate: **RSA** or **Elliptic Curve DSA** (ECDSA). ECDSA uses smaller key sizes than the RSA algorithm and, therefore, provides a performance enhancement for processing SSL/TLS connections. ECDSA also provides equal or greater security than RSA. ECDSA is recommended for client browsers and operating systems that support it but you may be required to select RSA for compatibility with legacy browsers and operating systems. *Firewalls running PAN-OS 6.1 or earlier releases will delete any ECDSA certificates that you push from Panorama and any RSA certificates signed by an ECDSA certificate authority (CA) will be invalid on those firewalls.* You cannot use a hardware security module (HSM) to store private ECDSA keys used for SSL Forward Proxy or Inbound Inspection decryption.
Number of Bits	Select the key length for the certificate. If the firewall is in FIPS-CC mode and the key generation **Algorithm** is **RSA**, the RSA keys generated must be **2048** or **3027** bits. If the **Algorithm** is **Elliptic Curve DSA**, both key length options (**256** and **384**) work.
Digest	Select the **Digest** algorithm for the certificate. The available options depend on the key generation **Algorithm**: • **RSA**—**MD5**, **SHA1**, **SHA256**, **SHA384**, or **SHA512** • **Elliptic Curve DSA**—**SHA256** or **SHA384** If the firewall is in FIPS-CC mode and the key generation **Algorithm** is **RSA**, you must select **SHA256**, **SHA384**, or **SHA512** as the **Digest** algorithm. If the **Algorithm** is **Elliptic Curve DSA**, both **Digest** algorithms (**SHA256** and **SHA384**) work. *Client certificates that are used when requesting firewall services that rely on TLSv1.2 (such as administrator access to the web interface) cannot have SHA512 as a digest algorithm. The client certificates must use a lower digest algorithm (such as SHA384) or you must limit the Max Version to TLSv1.1 when you configure SSL/TLS service profiles for the firewall services (see Device > Certificate Management > SSL/TLS Service Profile).*
Expiration (days)	Specify the number of days (default is 365) that the certificate will be valid. *If you specify a Validity Period in a GlobalProtect satellite configuration, that value will override the value entered in this field.*
Certificate Attributes	**Add** additional **Certificate Attributes** to identify the entity to which you are issuing the certificate. You can add any of the following attributes:

Settings to Generate a Certificate	Description
	Country, **State**, **Locality**, **Organization**, **Department**, and **Email**. In addition, you can specify one of the following Subject Alternative Name fields: **Host Name** (SubjectAltName:DNS), **IP** (SubjectAltName:IP), and **Alt Email** (SubjectAltName:email). *To add a country as a certificate attribute, select Country from the Type column and then click into the Value column to see the ISO 6366 Country Codes.*

If you configured a hardware security module (HSM), the private keys are stored on the external HSM storage, not on the firewall.

Other Supported Actions to Manage Certificates

After you generate the certificate, its details display on the page and the following actions are available:

Other Supported Actions to Manage Certificates	Description
Delete	Select the certificate and **Delete** it. *If the firewall has a decryption policy, you cannot delete a certificate for which usage is set to Forward Trust Certificate or Forward Untrust Certificate. To change the certificate usage, see* Manage Default Trusted Certificate Authorities.
Revoke	Select the certificate that you want to revoke, and click **Revoke**. The certificate will be instantly set to revoked status. No commit is required.
Renew	In case a certificate expires or is about to expire, select the corresponding certificate and click **Renew**. Set the validity period (in days) for the certificate and click **OK**. If the firewall is the CA that issued the certificate, the firewall replaces it with a new certificate that has a different serial number but the same attributes as the old certificate. If an external certificate authority (CA) signed the certificate and the firewall uses the Online Certificate Status Protocol (OCSP) to verify certificate revocation status, the firewall uses the OCSP responder information to update the certificate status
Import	**Import** a certificate and configure as follows: • Enter Certificate Name to identify the certificate. • Browse to the certificate file. If you import a **PKCS12**certificate and private key, a single file contains both. If you import a **PEM** certificate, the file contains only the certificate.

Other Supported Actions to Manage Certificates	Description
	• Select the **File Format** for the certificate. • Select **Private key resides on Hardware Security Module** if an HSM stores the key for this certificate. For HSM details, see Device > Setup > HSM. • **Import Private Key** as needed (PEM format only). If you selected **PKCS12**as the certificate **File Format**, the selected **Certificate File** includes the key. If you selected the **PEM** format, browse to the encrypted private key file (generally named *.key). For both formats, enter the **Passphrase** and **Confirm Passphrase**. When you import a certificate and select **Import Private Key**, select **Block Private Key Export** to prevent any administrators, including Superusers, from exporting the private key. *When you import a certificate to a Palo Alto Networks firewall or Panorama server that is in FIPS-CC mode, you must import the certificate as a Base64-Encoded Certificate (PEM) and you must encrypt the private key with AES. Also, you must use SHA1 as the passphrase-based key derivation method.* To import a PKCS12 certificate, convert the certificate to the PEM format (using a tool such as OpenSSL); ensure that the password phrase you use during conversion is at least six characters.
Export	Select the certificate you want to export, click **Export**, and select a **File Format**: • Encrypted Private Key and Certificate (PKCS12)—The exported file will contain both the certificate and private key. • Base64 Encoded Certificate (PEM)—If you want to export the private key also, select Export Private Key and enter a Passphrase and Confirm Passphrase. • Binary Encoded Certificate (DER)—You can export only the certificate, not the key: ignore Export Private Key and passphrase fields.
Import HA Key Export HA Key	The HA keys must be swapped across both the firewalls peers; that is the key from firewall 1 must be exported and then imported in to firewall 2 and vice versa. To import keys for high availability (HA), click **Import HA Key** and **Browse** to specify the key file for import. To export keys for HA, click **Export HA Key** and specify a location to save the file.
Define the usage of the certificate	In the Name column, select the certificate and then select options appropriate for how you plan to use the certificate.
PDF/CSV	Administrative roles with a minimum of read-only access can export the managed certificate configuration table as **PDF/CSV**. You can apply filters to create more specific table configuration outputs for things such as

Other Supported Actions to Manage Certificates	Description
	audits. Only visible columns in the web interface will be exported. See Configuration Table Export.

Manage Default Trusted Certificate Authorities

- Device > Certificate Management > Certificates > Default Trusted Certificate Authorities

Use this page to view, disable, or export, the pre-included certificate authorities (CAs) that the firewall trusts. The pre-installed list of CAs includes the most common and trusted certificate providers responsible for issuing the certificates the firewall requires to secure connections to the internet. For each trusted root CA, the name, subject, issuer, expiration date and validity status are displayed.

The firewall does not trust intermediate CAs by default because intermediate CAs are not a part of the chain of trust between the firewall and the trusted root CA. You must manually add any intermediate CAs that you want the firewall to trust, along with any additional trusted enterprise CAs that your organization requires (**Device** > **Certificate Management** > **Certificates** > **Device Certificates**).

Trusted Certificate Authorities Settings	Description
Enable	If you disabled a CA, you can re-**Enable** it.
Disable	Select the CA and **Disable** it. You might use this option to trust only specific CAs or to disable all other CAs and trust only your local CA.
Export	Select and **Export** the CA certificate. You can import into another system or view the certificate offline.

Device > Certificate Management > Certificate Profile

- **Device** > **Certificate Management** > **Certificate Profile**
- **Panorama** > **Certificate Management** > **Certificate Profile**

Certificate profiles define which certificate authority (CA) certificates to use for verifying client certificates, how to verify certificate revocation status, and how that status constrains access. You select the profiles when configuring certificate authentication for Authentication Portal, GlobalProtect, site-to-site IPSec VPN, Dynamic DNS (DDNS), and web interface access to firewalls and Panorama. You can configure a separate certificate profile for each of these services.

Certificate Profile Settings	Description
Name	(Required) Enter a name to identify the profile (up to 63 characters on the firewall or up to 31 characters on Panorama). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Username Field	If GlobalProtect only uses certificates for portal and gateway authentication, the PAN-OS software uses the certificate field you select in the **Username Field** drop-down as the username and matches it to the IP address for the User-ID service: • **Subject**—The common name. • **Subject Alt**—The Email or Principal Name. • **None**—Typically for GlobalProtect device or pre-login authentication.
Domain	Enter the NetBIOS domain so the PAN-OS software can map users through User-ID.
CA Certificates	(Required) **Add** a **CA Certificate** to assign to the profile. Optionally, if the firewall uses Online Certificate Status Protocol (OCSP) to verify certificate revocation status, configure the following fields to override the default behavior. For most deployments, these fields do not apply. • By default, the firewall uses the Authority Information Access (AIA) information from the certificate to extract the OCSP responder information. To override the AIA information, enter a **Default OCSP URL** (starting with **`http://`** or **`https://`**). • By default, the firewall uses the certificate selected in the **CA Certificate** field to validate OCSP responses. To use a different

Certificate Profile Settings	Description
	certificate for validation, select it in the **OCSP Verify CA Certificate** field. In addition, enter a **Template Name** to identify the template that was used to sign the certificate.
Use CRL	Select this option to use a certificate revocation list (CRL) to verify the revocation status of certificates.
Use OCSP	Select this option to use OCSP to verify the revocation status of certificates. *If you select both OCSP and CRL, the firewall first tries OCSP and only falls back to the CRL method if the OCSP responder is unavailable.*
CRL Receive Timeout	Specify the interval (1 to 60 seconds) after which the firewall stops waiting for a response from the CRL service.
OCSP Receive Timeout	Specify the interval (1 to 60 seconds) after which the firewall stops waiting for a response from the OCSP responder.
Certificate Status Timeout	Specify the interval (1 to 60 seconds) after which the firewall stops waiting for a response from any certificate status service and applies any session blocking logic you define.
Block session if certificate status is unknown	Select this option if you want the firewall to block sessions when the OCSP or CRL service returns a certificate revocation status of *unknown*. Otherwise, the firewall proceeds with the sessions.
Block sessions if certificate status cannot be retrieved within timeout	Select this option if you want the firewall to block sessions after it registers an OCSP or CRL request timeout. Otherwise, the firewall proceeds with the sessions.
Block sessions if the certificate was not issued to the authenticating device	(GlobalProtect only) Select this option if you want the firewall to block sessions when the serial number attribute in the subject of the client certificate does not match the host ID that the GlobalProtect app reports for the endpoint. Otherwise, the firewall allows the sessions. This option applies only to GlobalProtect certificate authentication.

Device > Certificate Management > OCSP Responder

Select **Device** > **Certificate Management** > **OCSP Responder** to define an Online Certificate Status Protocol (OCSP) responder (server) to verify the revocation status of certificates.

Besides adding an OCSP responder, enabling OCSP requires the following tasks:

- Enable communication between the firewall and the OCSP server: select **Device** > **Setup** > **Management**, select **HTTP OCSP** in Management Interface Settings, and then click **OK**.
- If the firewall will decrypt outbound SSL/TLS traffic, optionally configure it to verify the revocation status of destination server certificates: select **Device** > **Setup** > **Sessions**, click **Decryption Certificate Revocation Settings**, select **Enable** in the OCSP settings, enter the **Receive Timeout** (the interval after which the firewall stops waiting for an OCSP response), and then click **OK**.
- Optionally, to configure the firewall as an OCSP responder, add an Interface Management profile to the interface used for OCSP services. First, select **Network** > **Network Profiles** > **Interface Mgmt**, click **Add**, select **HTTP OCSP**, and then click **OK**. Second, select **Network** > **Interfaces**, click the name of the interface that the firewall will use for OCSP services, select **Advanced** > **Other info**, select the Interface Management profile you configured, and then click **OK** and **Commit**.

Enable an OCSP responder so that if a certificate was revoked, you are notified and can take appropriate action to establish a secure connection to the portal and gateways.

OCSP Responder Settings	Description
Name	Enter a name to identify the responder (up to 31 characters). The name is case-sensitive. It must be unique and use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the responder is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared. After you save the responder, you can't change its **Location**.
Host Name	Enter the host name (recommended) or IP address of the OCSP responder. From this value, PAN-OS automatically derives a URL and adds it to the certificate being verified. If you configure the firewall as an OCSP responder, the host name must resolve to an IP address in the interface that the firewall uses for OCSP services.

Device > Certificate Management > SSL/TLS Service Profile

- Device > Certificate Management > SSL/TLS Service Profile
- Panorama > Certificate Management > SSL/TLS Service Profile

SSL/TLS service profiles specify a server certificate and a protocol version or range of versions for firewall or Panorama services that use SSL/TLS (such as administrative access to the web interface). By defining the protocol versions, the profiles enable you to restrict the cipher suites that are available for securing communication with the client systems requesting the services.

In the client systems that request firewall or Panorama services, the certificate trust list (CTL) must include the certificate authority (CA) certificate that issued the certificate specified in the SSL/TLS service profile. Otherwise, users will see a certificate error when requesting the services. Most third-party CA certificates are present by default in client browsers. If an enterprise or firewall-generated CA certificate is the issuer, you must deploy that CA certificate to the CTL in client browsers.

To add a profile, click **Add**, complete the fields in the following table.

SSL/TLS Service Profile Settings	Description
Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive. It must be unique and use only letters, numbers, spaces, hyphens, and underscores.
Shared	If the firewall has more than one virtual system (vsys), selecting this option makes the profile available on all virtual systems. By default, this option is cleared and the profile is available only for the vsys selected in the **Device** tab, **Location** drop-down.
Certificate	Select, import, or generate a server certificate to associate with the profile (see Manage Firewall and Panorama Certificates). *Do not use certificate authority (CA) certificates for SSL/TLS services; use only signed certificates.*
Min Version Max Version	Select the earliest (**Min Version**) and latest (**Max Version**) version of TLS that services can use: **TLSv1.0**, **TLSv1.1**, **TLSv1.2**, **TLSv1.3**, or **Max** (the latest available version). *On firewalls in FIPS/CC mode running PAN-OS 8.0 or a later release, TLSv1.1 is the earliest supported TLS version; do not select TLSv1.0.* *Client certificates that are used when requesting firewall services that rely on TLSv1.2 cannot have SHA512 as a digest algorithm. The client certificates must use a lower digest algorithm (such as SHA384) or you must limit the Max Version to TLSv1.1 for the services.*

SSL/TLS Service Profile Settings	Description
	 *Use the strongest version of the protocol you can to provide the strongest security for your network. If you can, set the Min Version to TLSv1.2 and set the Max Version to Max.*

Device > Certificate Management > SCEP

The simple certificate enrollment protocol (SCEP) provides a mechanism for issuing a unique certificate to endpoints, gateways, and satellite devices. Select **Device** > **Certificate Management** > **SCEP** to create an SCEP configuration.

For more information on how to create a SCEP profile, refer to Deploying Certificates Using SCEP

.

To start a new SCEP configuration, click **Add** and then complete the following fields.

SCEP Settings	Description
Name	Specify a descriptive Name to identify this SCEP configuration, such as SCEP_*Example*. This name distinguishes a SCEP profile from other instances that you might have among the configuration profiles.
Location	Select a Location for the profile if the system has multiple virtual systems. The location identifies where the SCEP configuration is available.
One Time Password (Challenge)	
SCEP Challenge	(Optional) To make SCEP-based certificate generation more secure, you can configure a SCEP challenge-response mechanism (a one-time password (OTP)) between the public key infrastructure (PKI) and the portal for each certificate request. *After you configure this mechanism, its operation is invisible, and no further input from you is necessary.* The challenge mechanism that you select determines the source of the OTP. If you select **Fixed**, copy the enrollment challenge password from the SCEP server for the PKI and enter the string in the portal's **Password** dialog that displays when configured as **Fixed**. Each time the portal requests a certificate, it uses this password to authenticate with the PKI. If you select **Dynamic**, you enter the username and password of your choice (possibly the credentials of the PKI administrator) and the SCEP **Server URL** where the portal-client submits these credentials. This username and password remains the same while the SCEP server transparently generates an OTP password for the portal upon each certificate request. (You can see this OTP change after a screen refresh in "The enrollment challenge password is" field upon each certificate request.) The PKI transparently passes each new password to the portal, which then uses the password for its certificate request. *To comply with the U.S. Federal Information Processing Standard (FIPS), select Dynamic, specify a Server URL that uses HTTPS, and enable SCEP Server SSL*

SCEP Settings	Description
	Authentication. (FIPS-CC operation is indicated on the firewall login page and in the firewall status bar.)
Configuration	
Server URL	Enter the URL at which the portal requests and receives client certificates from the SCEP server. Example: `http://<hostname or IP>/certsrv/mscep/.`
CA-IDENT Name	Enter a string to identify the SCEP server. Maximum length is 255 characters.

Subject	Configure the Subject to include identifying information about the device and optionally user and provide this information in the certificate signing request (CSR) to the SCEP server.
	When used to request client certificates for endpoints, the endpoint sends identifying information about the device that includes its host ID value. The host ID value varies by device type, either GUID (Windows) MAC address of the interface (Mac), Android ID (Android devices), UDID (iOS devices), or a unique name that GlobalProtect assigns (Chrome). When used to request certificates for satellite devices, the host ID value is the device serial number.
	To specify additional information in the CSR, enter the Subject name. The subject must be a distinguished name in the <*attribute*>=<*value*> format and must include the common name (CN) key. For example:
	`O=acme,CN=acmescep`
	There are two ways to specify the CN:
	• (Recommended) **Token-based CN**—Enter one of the supported tokens **$USERNAME**, **$EMAILADDRESS**, or **$HOSTID**. Use the username or email address variable to ensure that the portal requests certificates for a specific user. To request certificates for the device only, specify the hostid variable. When the GlobalProtect portal pushes the SCEP settings to the agent, the CN portion of the subject name is replaced with the actual value (username, hostid, or email address) of the certificate owner. For example:
	`O=acme,CN=$HOSTID`
	• **Static CN**—The CN you specify will be used as the subject for all certificates issued by the SCEP server. For example:
	`O=acme,CN=acmescep`

Subject Alternative Name Type	After you select a type other than **None**, a dialog displays for you to enter the appropriate value:

SCEP Settings	Description
	• **RFC 822 Name**—Enter the email name in a certificate's subject or Subject Alternative Name extension. • **DNS Name**—Enter the DNS name used to evaluate certificates. • **Uniform Resource Identifier (URI)**—Enter the name of the URI resource from which the client obtains the certificate.
Cryptographic Settings	• **Number of Bits**—Select the key's **Number of Bits** for the certificate. If the firewall is in FIPS-CC mode, the generated keys must be at least 2,048 bits. (FIPS-CC operation is indicated on the firewall login page and the firewall status bar.) • **Digest**—Select the **Digest** algorithm for the certificate: **SHA1**, **SHA256**, **SHA384**, or **SHA512**. If the firewall is in FIPS-CC mode, you must select **SHA256**, **SHA384**, or **SHA512** as the **Digest** algorithm.
Use as digital signature	Select this option to configure the endpoint to use the private key in the certificate to validate a digital signature.
Use for key encipherment	Select this option to configure the client endpoint to use the private key in the certificate to encrypt data exchanged over the HTTPS connection established with the certificates issued by the SCEP server.
CA Certificate Fingerprint	(Optional) To ensure that the portal connects to the correct SCEP server, enter the **CA Certificate Fingerprint**. Obtain this fingerprint from the SCEP server interface in the **Thumbprint** field. Log in to the SCEP server's administrative user interface (for example, at http://<hostname or IP>/CertSrv/mscep_admin/). Copy the thumbprint and enter it in **CA Certificate Fingerprint**.
SCEP Server SSL Authentication	To enable SSL, select the root **CA Certificate** for the SCEP server. Optionally, you can enable mutual SSL authentication between the SCEP server and the GlobalProtect portal by selecting a **Client Certificate**.

Device > Certificate Management > SSL Decryption Exclusion

View and manage SSL decryption exclusions. There are two types of decryption exclusions, predefined exclusions and custom exclusions:

- Predefined decryption exclusions allow applications and services that might break when the firewall decrypts them to remain encrypted. Palo Alto Networks defines the predefined decryption exclusions and delivers updates and additions to the predefined exclusions list at regular intervals as part of the applications and threats content update. Predefined exclusions are enabled by default, but you can choose to disable the exclusion as needed.
- You can create custom decryption exclusions to exclude server traffic from decryption. All traffic originating from or destined to the targeted server remains encrypted.

You can also exclude traffic from decryption based on application, source, destination, URL category, and service.

Use the settings on this page to Modify or Add a Decryption Exclusion and to Manage Decryption Exclusions.

SSL Decryption Exclusions Settings	Description
Modify or **Add** a Decryption Exclusion	
Hostname	Enter a **Hostname** to define a custom decryption exclusion. The firewall compares the hostname to the SNI requested by the client or to the CN presented in the server certificate. The firewall excludes sessions in which the server presents a CN that contains the defined domain from decryption. You can use asterisks (*) as wildcards to create decryption exclusions for multiple hostnames associated with a domain. Asterisks behave the same way that carets (^) behave for URL category exceptions—each asterisk controls one variable subdomain (label) in the hostname. This enables you to create both very specific and very general exclusions. For example: • mail.*.com matches mail.company.com but does not match mail.company.sso.com. • *.company.com matches tools.company.com but does not match eng.tools.company.com. • *.*.company.com matches eng.tools.company.com but does not match eng.company.com. • *.*.*.company.com matches corp.exec.mail.company.com, but does not match corp.mail.company.com. • mail.google.* matches mail.google.com, but does not match mail.google.uk.com. • mail.google.*.* matches mail.google.co.uk, but does not match mail.google.com.

SSL Decryption Exclusions Settings	Description
	For example, to use wildcards to exclude video-stats.video.google.com from decryption but not to exclude video.google.com from decryption, exclude *.*.google.com. *Regardless of the number of asterisk wildcards that precede a hostname (without a non-wildcard label preceding the hostname), the hostname matches the entry. For example, *.google.com, *.*.google.com, and *.*.*.google.com all match google.com. However, *.dev.*.google.com does not match google.com because one label (dev) is not a wildcard.* Hostnames should be unique for each entry—if a predefined entry is delivered to the firewall that matches an existing custom entry, the custom entry takes precedence. You cannot edit the Hostname for a predefined decryption exclusion.
Shared	Select **Shared** to share a decryption exclusion across all virtual systems in a multiple virtual system firewall. While predefined decryption exclusions are shared by default, you can enable and disable both predefined and custom entries for a specific virtual system.
Description	(Optional) Describe the application that you are excluding from decryption, including why the application breaks when decrypted.
Exclude	Exclude the application from decryption. Disable this option to start decrypting an application that was previously excluded from decryption.
Manage Decryption Exclusions	
Enable	**Enable** one or more entries to exclude them from decryption.
Disable	**Disable** one or more predefined decryption exclusions. Because decryption exclusions identify applications that break when decrypted, disabling one of these entries will cause the application to be unsupported. The firewall will attempt to decrypt the application and the application will break. You can use this option if you want to ensure certain encrypted applications do not enter your network.
Show obsoletes	**Show obsoletes** to view predefined entries that Palo Alto Networks no longer defines as decryption exclusions. **More about obsolete entries:** Updates to predefined decryption exclusions (including the removal of a predefined entry) are delivered to the firewall as part of Applications and Threats content updates. Predefined entries with **Exclude from decryption** enabled are automatically removed from the list of SSL decryption exclusions when the firewall receives a content update that no longer includes that entry. However, predefined entries with **Exclude from decryption** disabled remain on the SSL decryption list even after the firewall receives a content update

SSL Decryption Exclusions Settings	Description
	that no longer includes that entry. When you **Show obsoletes**, you will see these disabled predefined entries that are not currently being enforced; you can remove these entries manually as needed.
Show Local Exclusion Cache	**Show Local Exclusion Cache** displays the sites that the firewall automatically excluded from decryption because of technical circumstances that prevent decryption, such as pinned certificates, client authentication, or unsupported ciphers. The Local SSL Decryption Cache differs from the SSL Decryption Exclusion List (**Device** > **Certificate Management** > **SSL Decryption Exclusion**), which contains the sites that prevent decryption that Palo Alto Networks has identified and to which you can add permanent decryption exclusions that you choose to make. The the firewall populates the Local SSL Decryption Cache with locally discovered decryption exceptions, based on the settings of the Decryption profile associated with the Decryption policy rule that controls the traffic. Excluded sites remain in the local cache for 12 hours and then age out. Each exclusion entry includes information about the application, the server, the reason why the firewall automatically excluded the site from decryption, the Decryption profile applied to the traffic, and the Vsys.

Device > Certificate Management > SSH Service Profile

SSH service profiles enable you to restrict the cipher, key exchange, and message authentication code algorithms that encrypt and protect the integrity of your data. Specifically, these profiles strengthen data protection during SSH sessions between your command line interface (CLI) and the management connections and high availability (HA) appliances on your network. You can also generate a new SSH host key and specify the thresholds (data volume, time interval, and packet count) that initiate an SSH rekey.

To configure an SSH service profile, **Add** an HA or Management - Server profile, complete the fields in the following table as appropriate, and then click **OK** and **Commit** your changes.

The process for applying a profile differs between the profile types.

- To apply an HA profile, select Device > High Availability > General. Under SSH HA Profile Setting, select an existing profile. Click **OK** and **Commit** your changes.
- To apply a Management - Server profile, select Device > Setup > Management. Under SSH Management Profiles Settings, select an existing profile. Click **OK** and **Commit** your changes.

After applying a profile, you must perform an SSH service restart from your CLI to activate the profile.

SSH Service Profile Settings	Description
Name	Enter a name for the profile (up to 31 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores.
Ciphers	Select the cipher algorithms your server will support for SSH session encryption.
KEX	Select the key exchange algorithms your server will support during an SSH session.
MAC	Select the message authentication code algorithms your server will support during an SSH session.
Hostkey	Select a host key type and key length to generate a new key pair of the specified host key algorithm and key length. *After you select a host key type, you can enter a key length. The default key type and length is RSA 2048.*
Data	Set the maximum volume of data (in megabytes) transmitted before an SSH rekey (range is 10 to 4000; default is the value of the cipher you selected).

SSH Service Profile Settings	Description
Interval	Set the maximum time interval (in seconds) before an SSH rekey (range is 10 to 3600; default is no time-based rekeying).
Packets	Set the maximum number of packets (2^n) before an SSH rekey. *If you do not configure this parameter, the session will rekey after 2^{28} packets. To ensure a more frequent rekey, specify a value in the range 12 to 27.*

Device > Response Pages

Custom response pages are the web pages that display when a user tries to access a URL. You can provide a custom HTML message that is downloaded and displayed instead of the requested web page or file.

Each virtual system can have its own custom response pages. The following table describes the types of custom response pages that support customer messages.

Custom Response Page Types	Description
Antivirus Block Page	Access blocked due to a virus infection.
Application Block Page	Access blocked because the application is blocked by a Security policy rule.
Authentication Portal Comfort Page	The firewall displays this page so that users can enter login credentials to access services that are subject to Authentication policy rules (see Policies > Authentication). Enter a message that tells users how to respond to this authentication challenge. The firewall authenticates users based on the **Authentication Profile** specified in the authentication enforcement object assigned to an Authentication rule (see Objects > Authentication).  *You can display unique authentication instructions for each Authentication rule by entering a Message in the associated authentication enforcement object. The message defined in the object overrides the message defined in the Authentication Portal Comfort Page.*
Data Filtering Block Page	Content was matched against a data filtering profile and blocked because sensitive information was detected.
File Blocking Continue Page	Page for users to confirm that downloading should continue. This option is available only if Continue functionality is enabled in the security profile. Select Objects > Security Profiles > File Blocking.
File Blocking Block Page	Access blocked because access to the file is blocked.
GlobalProtect App Help Page	Custom help page for GlobalProtect users (accessible from the settings menu on the GlobalProtect status panel).
GlobalProtect Portal Login Page	Login page for users who attempt to authenticate to the GlobalProtect portal webpage.
GlobalProtect Portal Home Page	Home page for users who successfully authenticate to the GlobalProtect portal webpage.
GlobalProtect App Welcome Page	Welcome page for users who successfully connect to GlobalProtect.
MFA Login Page	The firewall displays this page so that users can respond to multi-factor authentication (MFA) challenges when accessing services

Custom Response Page Types	Description
	that are subject to Authentication policy rules (see Policies > Authentication). Enter a message that tells users how to respond to the MFA challenges.
SAML Auth Internal Error Page	Page to inform users that SAML authentication failed. The page includes a link for the user to retry authentication.
SSL Certificate Errors Notify Page	Notification that an SSL certificate has been revoked.
SSL Decryption Opt-out Page	User warning page indicating that the firewall will decrypt SSL sessions for inspection.
URL Filtering and Category Match Block Page	Access blocked by a URL filtering profile or because the URL category is blocked by a Security policy rule.
URL Filtering Continue and Override Page	Page with initial block policy that allows users to bypass the block. For example, a user who thinks the page was blocked inappropriately can click **Continue** to proceed to the page. With the override page, a password is required for the user to override the policy that blocks this URL. See the URL Admin Override section for instructions on setting the override password.
URL Filtering Safe Search Enforcement Block Page	Access blocked by a Security policy rule with a URL filtering profile that has the **Safe Search Enforcement** option enabled. The user sees this page if a search is performed using Bing, Google, Yahoo, Yandex, or YouTube and their browser or search engine account setting for Safe Search is not set to strict. The block page will instruct the user to set the Safe Search setting to strict.
Anti Phishing Block Page	Displays to users when they attempt to enter valid corporate credentials (usernames or passwords) on a web page for which credential submissions are blocked. The user can continue to access the site but remains unable to submit valid corporate credentials to any associated web forms. Select Objects > Security Profiles > URL Filtering to enable credential detection and control credential submissions to web pages based on URL category.
Anti Phishing Continue Page	This page warns users against submitting corporate credentials (usernames and passwords) to a web site. Warning users against submitting credentials can help to discourage them from reusing corporate credentials and to educate them about possible phishing attempts. Users see this page when they attempt to submit credentials to a site for which the **User Credential Submission** permissions are set to **continue** (see Objects > Security Profiles > URL Filtering). They must select **Continue** to enter credentials on the site.

You can perform any of the following functions for **Response Pages**.

- To import a custom HTML response page, click the link of the page type you would like to change and then click import/export. Browse to locate the page. A message is displayed to indicate whether the import succeeded. For the import to be successful, the file must be in HTML format.
- To export a custom HTML response page, click **Export** for the type of page. Select whether to open the file or save it to disk and, if appropriate, select **Always use the same option**.
- To enable or disable the **Application Block** page or **SSL Decryption Opt-out** pages, click **Enable** for the type of page. Select or deselect **Enable**, as appropriate.
- To use the default response page instead of a previously uploaded custom page, delete the custom block page and commit. This will set the default block page as the new active page.

Device > Log Settings

Select **Device** > **Log Settings** to configure alarms, clear logs, or enable log forwarding to Panorama, Logging Service, and other external services.

- Select Log Forwarding Destinations
- Define Alarm Settings
- Clear Logs

Select Log Forwarding Destinations

Device > **Log Settings**

The Log Settings page allows you to configure log forwarding to:

- **Panorama, SNMP trap receivers, email servers, Syslog servers, and HTTP servers**—You can also add or remove tags from a source or destination IP address in a log entry; all log types except System logs and Configuration logs support tagging.
- **Logging Service**—If you have a Logging Service subscription and have enabled the Logging Service (Device > Setup > Management), then the firewall will send the logs to the Logging Service when you configure log forwarding to Panorama/Logging Service. Panorama will query the Logging Service to access the logs, to display the logs, and to generate reports.
- **Azure Security Center**—The integration with Azure Security Center is available only for VM-Series firewalls on Azure.
  - If you launched the VM-Series firewall from Azure Security Center, a security policy rule with the log forwarding profiles is automatically enabled for you.
  - If you launched the VM-Series firewall from the Azure Marketplace or using custom Azure templates, you must manually select **Azure-Security-Center-Integration** to forward System logs, User-ID logs, and HIP Match logs to Azure Security Center and use the Log Forwarding profile for other log types (see Objects > Log Forwarding).

  The free tier of Security Center is automatically enabled on your Azure subscription.

You can forward the following log types: System, Configuration, User-ID, HIP Match, and Correlation logs. To specify destinations for each log type, **Add** one or more match list profiles (up to 64) and complete the fields described in the following table.

To forward Traffic, Threat, WildFire Submissions, URL Filtering, Data Filtering, Tunnel Inspection, GTP, and Authentication logs, you must configure a Log Forwarding profile (see Objects > Log Forwarding).

Match List Profile Settings	Description
Name	Enter a name (up to 31 characters) to identify the match list profile. A valid name must start with an alphanumeric character and can contain zeros, alphanumeric characters, underscores, hyphens, periods, or spaces.
Filter	By default, the firewall forwards **All Logs** of the type for which you add the match list profile. To forward a subset of the logs, open the drop-down and select an existing filter or select **Filter Builder** to add a new filter. For each query in a new filter, specify the following fields and **Add** the query:

Match List Profile Settings	Description
	• **Connector**—Select the connector logic (AND/OR) for the query. Select **Negate** if you want to apply negation to the logic. For example, to avoid forwarding logs from an untrusted zone, select **Negate**, select **Zone** as the Attribute, select **equal** as the Operator, and enter the name of the untrusted Zone in the Value column. • **Attribute**—Select a log attribute. The available attributes vary by log type. • **Operator**—Select the criterion to determine whether the attribute applies (such as **equal**). The available criteria vary by the log type. • **Value**—Specify the attribute value to match. To display or export the logs that the filter matches, select **View Filtered Logs**. This tab provides the same options as the **Monitoring** tab pages (such as **Monitoring** > **Logs** > **Traffic**). *Set the filter to forward logs for all event severity levels (the default filter is All Logs). To create separate log forwarding methods for different severity levels, specify one or more severity levels in the Filter, configure a Forward Method, and then repeat the process for the rest of the severity levels.*
Description	Enter a description (up to 1,023 characters) to explain the purpose of this match list profile.
Panorama/Logging Service	Select **Panorama/Logging Service** if you want to forward logs to the Logging Service, Log Collectors or the Panorama management server. If you enable this option, you must configure log forwarding to Panorama. *You cannot forward Correlation logs from firewalls to Panorama. Panorama generates Correlation logs based on the firewall logs it receives.*
SNMP	**Add** one or more SNMP Trap server profiles to forward logs as SNMP traps (see Device > Server Profiles > SNMP Trap).
Email	**Add** one or more Email server profiles to forward logs as email notifications (see Device > Server Profiles > Email).
Syslog	**Add** one or more Syslog server profiles to forward logs as syslog messages (see Device > Server Profiles > Syslog).
HTTP	**Add** one or more HTTP server profiles to forward logs as HTTP requests (see Device > Server Profiles > HTTP).
Built-in Actions	You can select from two types of built-in actions when you **Add** an action to perform—Tagging and Integration. • **Tagging**—You can add an action for all log types that include a source or destination IP address in the log entry by configuring the following settings as needed.

Match List Profile Settings	Description
	You can tag only the source IP address in Correlation logs and HIP Match logs. You cannot configure any action for System logs and Configuration logs because the log type does not include an IP address in the log entry. • **Add** an action and enter a name to describe the action. • Select the IP address you want to automatically tag—**Source Address** or **Destination Address**. • Select the action—**Add Tag** or **Remove Tag**. • Select whether to register the IP address and tag mapping to the **Local User-ID** agent on this firewall or Panorama, or to a **Remote User-ID** agent. • To register the IP address and tag mapping to a **Remote User-ID** agent, select the HTTP server profile (Device > Server Profiles > HTTP) that will enable forwarding. • Configure the IP-Tag **Timeout** to set, in minutes, the amount of time that IP address-to-tag mapping is maintained. Setting the timeout to 0 means that the IP-Tag mapping does not timeout (range is 0 to 43200 (30 days); default is 0). *You can only configure a timeout with the Add Tag action.* • Enter or select the **Tags** you want to apply or remove from the target source or destination IP address. • **Integration**—Available only on the VM-Series firewall on Azure. **Add** a name and use this action to forward the selected logs to Azure Security Center. If you do not see this option, your Azure subscription may not be enabled for Azure Security Center. To add a device to the quarantine list based on the log forwarding profile filter, select **Quarantine**.

Define Alarm Settings

- Device > Log Settings

Use the Alarm Settings to configure Alarms for the CLI and the web interface. You can configure notifications for the following events:

- A security rule (or group of rules) has been matched at a specified threshold and within a specified time interval.
- Encryption/Decryption failure threshold is met.
- The Log database for each log type is nearing full; the quota by default is set to notify when 90% of the available disk space is used. Configuring alarms allows to take action before the disk is full, and logs are purged.

When you enable alarms, you can view the current list by clicking **Alarms** (

) in the bottom of the web interface.

To add an alarm, edit the Alarm Settings described in the following table.

Alarm Log Settings	Description
Enable Alarms	Alarms are visible only if you **Enable Alarms**. *If you disable alarms, the firewall does not alert you to critical events that require action. For example, an alarm tells you when the master key is about to expire; if the key expires before you change it, the firewall reboots into Maintenance mode and then requires a factory reset.*
Enable CLI Alarm Notifications	Enable CLI alarm notifications whenever alarms occur.
Enable Web Alarm Notifications	Open a window to display alarms on user sessions, including when they occur and when they are acknowledged.
Enable Audible Alarms	An audible alarm tone will play every 15 seconds on the administrator's computer when the administrator is logged into the web interface and unacknowledged alarms exist. The alarm tone will play until the administrator acknowledges all alarms. To view and acknowledge alarms, click **Alarms**. This feature is only available when the firewall is in FIPS-CC mode.
Encryption/Decryption Failure Threshold	Specify the number of encryption/decryption failures after which an alarm is generated.
<*Log-type*> Log DB	Generate an alarm when a log database reaches the indicated percentage of the maximum size.
Security Violations Threshold / Security Violations Time Period	An alarm is generated if a particular IP address or port hits a deny rule the specified number of times in the **Security Violations Threshold** setting within the period (seconds) specified in the **Security Violations Time Period** setting.
Violations Threshold / Violations Time Period / Security Policy Tags	An alarm is generated if the collection of rules reaches the number of rule limit violations specified in the **Violations Threshold** field during the period specified in the **Violations Time Period** field. Violations are counted when a session matches an explicit deny policy. Use **Security Policy Tags** to specify the tags for which the rule limit thresholds will generate alarms. These tags become available to be specified when defining security policies.
Selective Audit	The selective audit options are only available when the firewall is in FIPS-CC mode. Specify the following settings: • **FIPS-CC Specific Logging**—Enables verbose logging required for Common Criteria (CC) compliance. • **Packet Drop Logging**—Logs packets dropped by the firewall. • **Suppress Login Success Logging**—Stops logging of successful administrator logins to the firewall.

Alarm Log Settings	Description
	• **Suppress Login Failure Logging**—Stops logging of failed administrator logins to the firewall. • **TLS Session Logging**—Logs the establishment of TLS sessions. • **CA (OCSP/CRL) Session Establishment Logging**—Logs session establishment between the firewall and a certificate authority when the firewall sends a request to check certificate revocation status using the Online Certificate Status Protocol or a Certificate Revocation List server request. (Disabled by default.) • **IKE Session Establishment Logging**—Logs IPSec IKE session establishment when the VPN gateway on the firewall authenticates with a peer. The peer can be a Palo Alto Networks firewalls or another security device used to initiate and terminate VPN connections. The interface name that is specified in the log is the interface that is bound to the IKE gateway. The IKE gateway name is also displayed if applicable. Disabling this option stops logging of all IKE logging events. (Enabled by default.) • **Suppressed Administrators**—Stops logging of changes that the listed administrators make to the firewall configuration.

Clear Logs

- Device > Log Settings

You can clear logs on the firewall when you Manage Logs on the Log Settings page. Click the log type you want to clear and click **Yes** to confirm the request.

To automatically delete logs and reports, you can configure expiration periods. For details, see Logging and Reporting Settings.

Device > Server Profiles

The following topics describe server profile settings that you can configure on the firewall:

- Device > Server Profiles > SNMP Trap
- Device > Server Profiles > Syslog
- Device > Server Profiles > Email
- Device > Server Profiles > HTTP
- Device > Server Profiles > NetFlow
- Device > Server Profiles > RADIUS
- Device > Server Profiles > TACACS+
- Device > Server Profiles > LDAP
- Device > Server Profiles > Kerberos
- Device > Server Profiles > SAML Identity Provider
- Device > Server Profiles > DNS
- Device > Server Profiles > Multi Factor Authentication

Device > Server Profiles > SNMP Trap

Simple Network Management Protocol (SNMP) is a standard protocol for monitoring the devices on your network. To alert you to system events or threats on your network, monitored devices send SNMP traps to SNMP managers (trap servers). Select **Device** > **Server Profiles** > **SNMP Trap** or **Panorama** > **Server Profiles** > **SNMP Trap** to configure the server profile that enables the firewall or Panorama to send traps to the SNMP managers. To enable SNMP GET messages (statistics requests from an SNMP manager), see Enable SNMP Monitoring.

After creating the server profile, you must specify which log types will trigger the firewall to send SNMP traps (Device > Log Settings). For a list of the MIBs that you must load into the SNMP manager so it can interpret traps, see Supported MIBs.

Don't delete a server profile that any system log setting or logging profile uses.

SNMP Trap Server Profile Settings	Description
Name	Enter a name for the SNMP profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Version	Select the SNMP version: **V2c** (default) or **V3**. Your selection controls the remaining fields that the dialog displays. For either version, you can add up to four SNMP managers. *Use SNMPv3, which provides authentication and other features to keep network connections secure.*
For SNMP V2c	
Name	Specify a name for the SNMP manager. The name can have up to 31 characters that are alphanumeric, periods, underscores, or hyphens.
SNMP Manager	Specify the FQDN or IP address of the SNMP manager.
Community	Enter the community string, which identifies an SNMP *community* of SNMP managers and monitored devices and also serves as a password to authenticate the community members to each other during trap forwarding. The string can have up to 127 characters, accepts all characters, and is case-sensitive. *Don't use default community strings (don't set the community string to public or private). Use unique*

SNMP Trap Server Profile Settings	Description
	community strings, which avoids conflicts if you use multiple SNMP services. Because SNMP messages contain community strings in clear text, consider the security requirements of your network when defining community membership (administrator access).
For SNMP V3	
Name	Specify a name for the SNMP manager. The name can have up to 31 characters that are alphanumeric, periods, underscores, or hyphens.
SNMP Manager	Specify the FQDN or IP address of the SNMP manager.
User	Specify a username to identify the SNMP user account (up to 31 characters). The username you configure on the firewall must match the username configured on the SNMP manager.
EngineID	Specify the engine ID of the firewall. When an SNMP manager and the firewall authenticate to each other, trap messages use this value to uniquely identify the firewall. If you leave the field blank, the messages use the firewall serial number as the **EngineID**. If you enter a value, it must be in hexadecimal format, prefixed with 0x, and with another 10-128 characters to represent any number of 5-64 bytes (2 characters per byte). For firewalls in a high availability (HA) configuration, leave the field blank so that the SNMP manager can identify which HA peer sent the traps; otherwise, the value is synchronized and both peers will use the same **EngineID**.
Auth Password	Specify the authentication password of the SNMP user. The firewall uses the password to authenticate to the SNMP manager. The firewall uses Secure Hash Algorithm (SHA-1 160) to encrypt the password. The password must be 8–256 characters and all characters are allowed.
Priv Password	Specify the privacy password of the SNMP user. The firewall uses the password and Advanced Encryption Standard (AES-128) to encrypt traps. The password must be 8–256 characters and all characters are allowed.

Device > Server Profiles > Syslog

Select **Device** > **Server Profiles** > **Syslog** or **Panorama** > **Server Profiles** > **Syslog** to configure a server profile for forwarding firewall, Panorama, and Log Collector logs as syslog messages to a syslog server. To define a syslog server profile, click **Add** and specifying the New Syslog Server fields.

- *To select the Syslog Server profile for System, Config, User-ID, HIP Match, and Correlation logs, see Device > Log Settings.*
- *To select the Syslog Server Profile For Traffic, Threat, Wildfire, URL Filtering, Data Filtering, Tunnel Inspection, Authentication, and GTP logs, see Objects > Log Forwarding.*
- *You cannot delete a server profile that the firewall uses in any System or Config log settings or Log Forwarding profile.*

Syslog Server Settings	Description
Name	Enter a name for the syslog profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Servers Tab	
Name	Click **Add** and enter a name for the syslog server (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Server	Enter the IP address or FQDN of the syslog server.
Transport	Select whether to transport the syslog messages over UDP, TCP, or SSL. *Use SSL to encrypt and secure data sent to a syslog server. Data is sent over UDP or TCP in cleartext and is readable in transit.*
Port	Enter the port number of the syslog server (the standard port for UDP is 514; the standard port for SSL is 6514; for TCP you must specify a port number).
Format	Specify the syslog format to use: BSD (the default) or IETF.
Facility	Select one of the Syslog standard values. Select the value that maps to how your Syslog server uses the facility field to manage messages. For details on the facility field, see RFC 3164 (BSD format) or RFC 5424 (IETF format).
Custom Log Format Tab	

Syslog Server Settings	Description
Log Type	Click the log type to open a dialog box that allows you to specify a custom log format. In the dialog box, click a field to add it to the Log Format area. Other text strings can be edited directly in the Log Format area. Click **OK** to save the settings. View a description of each field that can be used for custom logs. For details on the fields that can be used for custom logs, see Device > Server Profiles > Email.
Escaping	Specify escape sequences. **Escaped characters** is a list of all the characters to be escaped without spaces.

Device > Server Profiles > Email

Select **Device** > **Server Profiles** > **Email** or **Panorama** > **Server Profiles** > **Email** to configure a server profile for forwarding logs as email notifications. To define an Email server profile, **Add** a profile and specify Email Notification Settings.

- *To select the Email Server profile for System, Config, User-ID, HIP Match, and Correlation logs, see Device > Log Settings.*
- *To select the Email Server Profile For Traffic, Threat, Wildfire, URL Filtering, Data Filtering, Tunnel Inspection, Authentication, and GTP logs, see Objects > Log Forwarding.*
- *You can also schedule email reports (Monitor > PDF Reports > Email Scheduler).*
- *You cannot delete a server profile that the firewall uses in any System or Config log settings or Log Forwarding profile.*

Email Notification Settings	Description
Name	Enter a name for the server profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location (Virtual systems only)	Select the scope in which the profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Servers Tab	
Name	Enter a name to identify the server (up to 31 characters). This field is just a label and does not have to be the host name of an existing email server.
Email Display Name	Enter the name shown in the **From** field of the email.
From	Enter the sender's email address, such as security_alert@company.com.
To	Enter the email address of the recipient.
Additional Recipient	Optionally, enter the email address of another recipient. You can only add one additional recipient. To add multiple recipients, add the email address of a distribution list.
Email Gateway	Enter the IP address or host name of the server that sends the email.
Protocol	Select the protocol you want to use to send the email (**Unauthenticated SMTP** or **SMTP over TLS**).
Port	Enter the port number you want to use to send the email if it differs from the default (25 for SMTP or 587 for TLS).
TLS Version	Select the TLS version you want to use (**1.2** or **1.1**).

Email Notification Settings	Description
(SMTP over TLS only)	*As a best practice, we strongly recommend using the latest TLS version.*
Authentication Method (SMTP over TLS only)	Select the authentication method you want to use: • **Auto** (default)—Allow the client and server to determine the authentication method. • **Login**—Use Base64 encoding for the username and password and transmit them separately. • **Plain**—Use Base64 encoding for the username and password and transmit them together.
Certificate Profile (SMTP over TLS only)	Select the certificate profile for the firewall to use to authenticate the email server.
Username (SMTP over TLS only)	Enter the username of the account that sends the email.
Password (SMTP over TLS only)	Enter the password of the account that sends the email.
Confirm Password (SMTP over TLS only)	Confirm the password of the account that sends the email.
Test Connection (SMTP over TLS only)	Confirm the connection between the email server and the firewall.
Custom Log Format Tab	
Log Type	Click the log type to open a dialog box that allows you to specify a custom log format. In the dialog box, click a field to add it to the Log Format area. Click **OK** to save your changes.
Escaping	Specify the **Escaped Characters** (all characters to not interpret literally) without spaces and specify the **Escape Character** for the escape sequence.

Device > Server Profiles > HTTP

Select **Device** > **Server Profiles** > **HTTP** or **Panorama** > **Server Profiles** > **HTTP** to configure a server profile for forwarding logs. You can configure the firewall to forward logs to an HTTP(S) destination, or to integrate with any HTTP-based service that exposes an API, and modify the URL, HTTP header, parameters, and the payload in the HTTP request to meet your needs. You can also use the HTTP server profile to access firewalls running the PAN-OS integrated User-ID agent and register one or more tags to a source or destination IP address on logs that a firewall generated.

To use the HTTP server profile to forward logs:

- *See* Device > Log Settings *for System, Config, User-ID, HIP Match, and Correlation logs.*
- *See* Objects > Log Forwarding *for Traffic, Threat, WildFire, URL Filtering, Data Filtering, Tunnel Inspection, Authentication, and GTP logs.*

You cannot delete an HTTP server profile if it is used to forward logs. To delete a server profile on the firewall or Panorama, you must delete all references to the profile from the Device > Log settings or Objects > Log Forwarding profile.

To define an HTTP server profile, **Add** a new profile and configure the settings in the following table.

HTTP Server Settings	Description
Name	Enter a name for the server profile (up to 31 characters). The name is case-sensitive and must be unique. A valid name must start with an alphanumeric character and can contain zeros, alphanumeric characters, underscores, hyphens, dots, or spaces.
Location	Select the scope in which the server profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change the **Location**.
Tag Registration	Tag registration allows you to add or remove a tag on a source or destination IP address in a log entry and register the IP address and tag mapping to the User-ID agent on a firewall using HTTP(S). You can then define dynamic address groups that use these tags as a filtering criteria to determine its members, and enforce policy rules to an IP address based on tags. **Add** the connection details to enable HTTP(S) access to the User-ID agent on a firewall. To register tags to the User-ID agent on Panorama, you do not need a server profile. Additionally, you cannot use the HTTP server profile to register tags to a User-ID agent running on a Windows server.
Servers Tab	
Name	**Add** an HTTP(s) server and enter a name (up to 31 characters) or remote User-ID agent. A valid name must be unique and start with an alphanumeric character; the name can contain zeros, alphanumeric characters, underscores, hyphens, dots, or spaces.

HTTP Server Settings	Description
	A server profile can include up to four servers.
Address	Enter the IP address of the HTTP(S) server. For tag registration, specify the IP address of the firewall configured as a User-ID agent.
Protocol	Select the protocol: HTTP or HTTPS.
Port	Enter the port number on which to access the server or firewall. The default port for HTTP is 80 and for HTTPS is 443. For tag registration, the firewall uses HTTP or HTTPS to connect to the web server on the firewalls that are configured as User-ID agents.
TLS Version	Select the TLS version supported for SSL on the server. The default is **1.2**.
Certificate Profile	Select the certificate profile to use for the TLS connection with the server. The firewall uses the specified certificate profile to validate the server certificate when establishing a secure connection to the server.
HTTP Method	Select the HTTP method that the server supports. The options are GET, PUT, POST (default), and DELETE. For the User-ID agent, use the GET method.
Username	Enter the username that has access privileges to complete the HTTP method you selected. If you are registering tags to the User-ID agent on a firewall, the username must be that of an administrator with a superuser role.
Password	Enter the password to authenticate to the server or the firewall.
Test Server Connection	Select a server and **Test Server Connection** to test network connectivity to the server. This test does not test connectivity to a server that is running the User-ID agent.
Payload Format Tab	
Log Type	The log type available for HTTP forwarding displays. Click the log type to open a dialog box that allows you to specify a custom log format.
Format	Displays whether the log type uses the default format, a predefined format, or a custom payload format that you defined.
Pre-defined Formats	Select the format for your service or vendor for sending logs. Predefined formats are pushed through content updates and can change each time you install a new content update on the firewall or Panorama.
Name	Enter a name for the custom log format.

HTTP Server Settings	Description
URI Format	Specify the resource to which you want to send logs using HTTP(S). If you create a custom format, the **URI** is the resource endpoint on the HTTP service. The firewall appends the URI to the IP address you defined earlier to construct the URL for the HTTP request. Ensure that the URI and payload format matches the syntax that your third-party vendor requires. You can use any attribute supported on the selected log type within the HTTP Header, Parameter, and Value pairs, and the request payload.
HTTP Headers	Add a Header and its corresponding value.
Parameters	Include the optional parameters and values.
Payload	Select the log attributes you want to include as the payload in the HTTP message to the external web server.
Send Test Log	Click this button to validate that the external web server receives the request and in the correct payload format.

Device > Server Profiles > NetFlow

Palo Alto Networks firewalls can export statistics about the IP traffic on their interfaces as NetFlow fields to a NetFlow collector. The NetFlow collector is a server you use to analyze network traffic for security, administration, accounting and troubleshooting. All Palo Alto Networks firewalls support NetFlow Version 9. The firewalls support only unidirectional NetFlow, not bidirectional. The firewalls perform NetFlow processing on all IP packets on the interfaces and do not support sampled NetFlow. You can export NetFlow records for Layer 3, Layer 2, virtual wire, tap, VLAN, loopback, and tunnel interfaces. For aggregate Ethernet interfaces, you can export records for the aggregate group but not for individual interfaces within the group. The firewalls support standard and enterprise (PAN-OS specific) NetFlow templates, which NetFlow collectors use to decipher the NetFlow fields. The firewalls select a template based on the type of exported data: IPv4 or IPv6 traffic, with or without NAT, and with standard or enterprise-specific fields.

To configure NetFlow exports, **Add** a NetFlow server profile to specify which NetFlow servers will receive the exported data and to specify export parameters. After you assign the profile to an interface (see Network > Interfaces), the firewall exports NetFlow data for all traffic on that interface to the specified servers.

Netflow Settings	Description
Name	Enter a name for the Netflow server profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Template Refresh Rate	The firewall periodically refreshes NetFlow templates to re-evaluate which one to use (in case the type of exported data changes) and to apply any changes to the fields in the selected template. Specify the rate at which the firewall refreshes NetFlow templates in **Minutes** (range is 1 to 3,600; default is 30) and **Packets** (exported records—range is 1 to 600; default is 20), according to the requirements of your NetFlow collector. The firewall refreshes the template after either threshold is passed. The required refresh rate depends on the NetFlow collector. If you add multiple NetFlow collectors to the server profile, use the value of the collector with the fastest refresh rate.
Active Timeout	Specify the frequency (in minutes) at which the firewall exports data records for each session (range is 1 to 60; default is 5). Set the frequency based on how often you want the NetFlow collector to update traffic statistics.
PAN-OS Field Types	Export PAN-OS specific fields for App-ID and the User-ID service in Netflow records.
Servers	
Name	Specify a name to identify the server (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Server	Specify the hostname or IP address of the server. You can add a maximum of two servers per profile.

Netflow Settings	Description
Port	Specify the port number for server access (default is 2055).

Device > Server Profiles > RADIUS

Select **Device** > **Server Profiles** > **RADIUS** or **Panorama** > **Server Profiles** > **RADIUS** to configure settings for the Remote Authentication Dial-In User Service (RADIUS) servers that authentication profiles reference (see Device > Authentication Profile). You can use RADIUS to authenticate end users who access your network resources (through GlobalProtect or Authentication Portal), to authenticate administrators defined locally on the firewall or Panorama, and to authenticate and authorize administrators defined externally on the RADIUS server.

RADIUS Server Settings	Description
Profile Name	Enter a name to identify the server profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Administrator Use Only	Select this option to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, this option appears only if the **Location** is **Shared**.
Timeout	Enter an interval in seconds after which an authentication request times out (range is 1–120, default is 3). *If you use the RADIUS server profile to integrate the firewall with an MFA service, enter an interval that gives users enough time to respond to the authentication challenge. For example, if the MFA service prompts for a one-time password (OTP), users need time to see the OTP on their endpoint device and then enter the OTP in the MFA login page.*
Authentication Protocol	Select the **Authentication Protocol** that the firewall uses to secure a connection to the RADIUS server: • **PEAP-MSCHAPv2**— (Default) Protected EAP (PEAP) with Microsoft Challenge-Handshake Authentication Protocol (MSCHAPv2) provides improved security over PAP or CHAP by transmitting both the username and password in an encrypted tunnel. • **PEAP with GTC**—Select Protected EAP (PEAP) with Generic Token Card (GTC) to use one-time tokens in an encrypted tunnel. • **EAP-TTLS with PAP**—Select EAP with Tunneled Transport Layer Security (TTLS) and PAP to transport plaintext credentials for PAP in an encrypted tunnel. • **CHAP**—Select Challenge-Handshake Authentication Protocol (CHAP) if the RADIUS server does not support EAP or PAP or is not configured for it.

RADIUS Server Settings	Description
	• **PAP**—Select Password Authentication Protocol (PAP) if the RADIUS server does not support EAP or CHAP or is not configured for it.
Allow users to change passwords after expiry	(PEAP-MSCHAPv2 with GlobalProtect 4.1 or later) Select this option to allow GlobalProtect users to change expired passwords.
Make Outer Identity Anonymous	(PEAP-MSCHAPv2, PEAP with GTC, or EAP-TTLS with PAP) This option is enabled by default to anonymize the user's identity in the outer tunnel that the firewall creates after authenticating with the server.  *Some RADIUS server configurations may not support anonymous outer IDs, and you may need to clear the option. When cleared, usernames are transmitted in cleartext.*
Certificate Profile	(PEAP-MSCHAPv2, PEAP with GTC, or EAP-TTLS with PAP) Select or configure a Certificate Profile to associate with the RADIUS server profile. The firewall uses the Certificate Profile to authenticate with the RADIUS server.
Retries	Specify the number of times to retry after a timeout (range is 1–5, default is 3).
Servers	Configure information for each server in the preferred order. • **Name**—Enter a name to identify the server. • **RADIUS Server**—Enter the server IP address or FQDN. • **Secret/Confirm Secret**—Enter and confirm a key to verify and encrypt the connection between the firewall and the RADIUS server. • **Port**—Enter the server port (range is 1–65,535, default is 1812) for authentication requests.

Device > Server Profiles > TACACS+

Select **Device** > **Server Profiles** > **TACACS+** or **Panorama** > **Server Profiles** > **TACACS+** to configure the settings that define how the firewall or Panorama connects to Terminal Access Controller Access-Control System Plus (TACACS+) servers (see Device > Authentication Profile). You can use TACACS+ to authenticate end users who access your network resources (through GlobalProtect or Authentication Portal), to authenticate administrators defined locally on the firewall or Panorama, and to authenticate and authorize administrators defined externally on the TACACS+ server.

TACACS+ Server Settings	Description
Profile Name	Enter a name to identify the server profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Administrator Use Only	Select this option to specify that only administrator accounts can use the profile for authentication. For multi-vsys firewalls, this option appears only if the **Location** is **Shared**.
Timeout	Enter an interval in seconds after which an authentication request times out (range is 1–20; default is 3).
Authentication Protocol	Select the **Authentication Protocol** that the firewall uses to secure a connection to the TACACS+ server: • **CHAP**—Challenge-Handshake Authentication Protocol (CHAP) is the default and preferred protocol because it is more secure than PAP. • **PAP**—Select Password Authentication Protocol (PAP) if the TACACS+ server does not support CHAP or is not configured for it. • **Auto**—The firewall first tries to authenticate using CHAP. If the TACACS+ server doesn't respond, the firewall falls back to PAP.
Use single connection for all authentication	Select this option to use the same TCP session for all authentications. This option improves performance by avoiding the processing required to initiate and tear down a separate TCP session for each authentication event.
Servers	Click **Add** and specify the following settings for each TACACS+ server: • **Name**—Enter a name to identify the server. • **TACACS+ Server**—Enter the IP address or FQDN of the TACACS+ server. • **Secret/Confirm Secret**—Enter and confirm a key to verify and encrypt the connection between the firewall and the TACACS+ server. • **Port**—Enter the server port (default is 49) for authentication requests.

Device > Server Profiles > LDAP

- **Device** > **Server Profiles** > **LDAP**
- **Panorama** > **Server Profiles** > **LDAP**

Add or select an LDAP Server Profile to configure settings for the Lightweight Directory Access Protocol (LDAP) servers that authentication profiles reference (see Device > Authentication Profile). You can use LDAP to authenticate end users who access your network resources (through GlobalProtect or Authentication Portal) and administrators defined locally on the firewall or Panorama.

LDAP Server Settings	Description
Profile Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Administrator Use Only	Select this option to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, this option appears only if the **Location** is **Shared**.
Use this profile for serial number check	Select this option to enable this LDAP server profile to collect serial numbers from managed endpoints. This information is used by the GlobalProtect portal and gateway to verify whether the endpoint is managed (serial number exists in the Active Directory) or not.
Server List	For each LDAP server, **Add** a host **Name**, IP address or FQDN (**LDAP Server**), and **Port** (default is 389).  *Configure at least two LDAP servers to provide redundancy.*
Type	Choose the server type from the drop-down.
Base DN	Specify the root context in the directory server to narrow the search for user or group information.
Bind DN	Specify the login name (Distinguished Name) for the directory server.  *The Bind DN account must have permission to read the LDAP directory.*
Password/Confirm Password	Specify the bind account password. The agent saves the encrypted password in the configuration file.

LDAP Server Settings	Description
Bind Timeout	Specify the time limit (in seconds) imposed when connecting to the directory server (range is 1 to 30; default is 30).
Search Timeout	Specify the time limit (in seconds) imposed when performing directory searches (range is 1 to 30; default is 30).
Retry Interval	Specify the interval (in seconds) after which the system will try to connect to the LDAP server after a previous failed attempt (range is 1 to 3,600; default is 60).
Require SSL/TLS secured connection	Select this option if you want the firewall to use SSL or TLS for communications with the directory server. The protocol depends on the server port: • 389 (default)—TLS (Specifically, the firewall uses the Start TLS operation, which upgrades the initial plaintext connection to TLS.) • 636—SSL • Any other port—The firewall first attempts to use TLS. If the directory server doesn't support TLS, the firewall falls back to SSL.  *This option is a best practice because it increases security and is selected by default.*
Verify Server Certificate for SSL sessions	Select this option (cleared by default) if you want the firewall to verify the certificate that the directory server presents for SSL/TLS connections. The firewall verifies the certificate in two respects: • The certificate is trusted and valid. For the firewall to trust the certificate, its root certificate authority (CA) and any intermediate certificates must be in the certificate store under **Device** > **Certificate Management** > **Certificates** > **Device Certificates**. • The certificate name must match the host **Name** of the LDAP server. The firewall first checks the certificate attribute Subject AltName for matching, then tries the attribute Subject DN. If the certificate uses the FQDN of the directory server, you must use the FQDN in the **LDAP Server** field for the name matching to succeed. If the verification fails, the connection fails. To enable this verification, you must also select **Require SSL/TLS secured connection**.  *Enable the firewall to verify the server certificate for SSL sessions to increase security.*

Device > Server Profiles > Kerberos

Select **Device** > **Server Profiles** > **Kerberos** or **Panorama** > **Server Profiles** > **Kerberos** to configure a server profile that enables users to natively authenticate to an Active Directory domain controller or a Kerberos V5-compliant authentication server. After configuring a Kerberos server profile you can assign it to an authentication profile (see Device > Authentication Profile). You can use Kerberos to authenticate end users who access your network resources (through GlobalProtect or Authentication Portal) and administrators defined locally on the firewall or Panorama.

To use Kerberos authentication, your back-end Kerberos server must be accessible over an IPv4 address. IPv6 addresses are not supported.

Kerberos Server Settings	Description
Profile Name	Enter a name to identify the server (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the profile is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Administrator Use Only	Select this option to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, this option appears only if the **Location** is **Shared**.
Servers	For each Kerberos server, click **Add** and specify the following settings: • **Name**—Enter a name for the server. • **Kerberos Server**—Enter the server IPv4 address or FQDN. • **Port**—Enter an optional port (range is 1 to 65,535; default is 88) for communication with the server.

Device > Server Profiles > SAML Identity Provider

Use this page to register a Security Assertion Markup Language (SAML) 2.0 identity provider (IdP) with the firewall or Panorama. Registration is a necessary step to enable the firewall or Panorama to function as a SAML service provider, which controls access to your network resources. When administrators and end users request resources, the service provider redirects the users to the IdP for authentication. The end users can be GlobalProtect or Authentication Portal users. The administrators can be managed locally on the firewall and Panorama or managed externally in the IdP identity store. You can configure SAML single sign-on (SSO) so that each user can automatically access multiple resources after logging into one. You can also configure SAML single logout (SLO) so that each user can simultaneously log out of every SSO-enabled service by logging out of any single service.

Authentication sequences don't support authentication profiles that specify SAML IdP server profiles.

In most cases, you cannot use SSO to access multiple apps on the same mobile device.

You cannot enable SLO for Authentication Portal users.

The easiest way to create a SAML IdP server profile is to **Import** a metadata file containing the registration information from the IdP. After saving a server profile with imported values, you can edit the profile to modify the values. If the IdP doesn't provide a metadata file, you can **Add** the server profile and manually enter the information. After creating a server profile, assign it to an authentication profile (see Device > Authentication Profile) for specific firewall or Panorama services.

SAML Identity Provider Server Settings	Description
Profile Name	Enter a name to identify the server (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the profile is available. In the context of a firewall that has multiple virtual systems, select a virtual system or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Administrator Use Only	Select this option to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, this option appears only if the **Location** is **Shared**.
Identity Provider ID	Enter an identifier for the IdP. Your IdP provides this information.
Identity Provider Certificate	Select the certificate that the IdP uses to sign SAML messages that it sends to the firewall. You must select an IdP certificate to ensure the integrity of messages that the IdP sends to the firewall. To validate the IdP certificate against the issuing Certificate Authority (CA), you must specify a **Certificate Profile** in any authentication profile that references the IdP server profile (see Device > Authentication Profile).

SAML Identity Provider Server Settings	Description
	When generating or importing a certificate and its associated private key, remember that the key usage attributes specified in the certificate control what you can use the key for. If the certificate explicitly lists key usage attributes, one of the attributes must be Digital Signature, which is not available in certificates that you generate on the firewall. In this case, you must Import the certificate and key from your enterprise certificate authority (CA) or a third-party CA. If the certificate doesn't specify key usage attributes, you can use the key for any purpose, including signing messages. In this case, you can use any method to obtain the certificate and key for signing SAML messages. IdP certificates support the following algorithms: • **Public key algorithms**—RSA (1,024 bits or larger) and ECDSA (all sizes). A firewall in FIPS/CC mode supports RSA (2,048 bits or larger) and ECDSA (all sizes). • **Signature algorithms**— SHA1, SHA256, SHA384, and SHA512. A firewall in FIPS/CC mode supports SHA256, SHA384, and SHA512.
Identity Provider SSO URL	Enter the URL that the IdP advertises for its single-sign on (SSO) service. If you create the server profile by importing a metadata file and the file specifies multiple SSO URLs, the firewall uses the first URL that specifies a POST or redirect binding method. *Palo Alto Networks strongly recommends using a URL that relies on HTTPS, although SAML also supports HTTP.*
Identity Provider SLO URL	Enter the URL that the IdP advertises for its single logout (SLO) service. If you create the server profile by importing a metadata file and the file specifies multiple SLO URLs, the firewall uses the first URL that specifies a POST or redirect binding method. *Palo Alto Networks strongly recommends using a URL that relies on HTTPS, although SAML also supports HTTP.*
SSO SAML HTTP Binding	Select the HTTP binding associated with the **Identity Provider SSO URL**. The firewall uses the binding to send SAML messages to the IdP. The options are: • **POST**—The firewall sends messages using base64-encoded HTML forms. • **Redirect**—The firewall sends base64-encoded and URL-encoded SSO messages within URL parameters. *If you import an IdP metadata file that has multiple SSO URLs, the firewall uses the binding of the first URL that uses the POST or redirect method. The firewall ignores URLs that use other bindings.*
SLO SAML HTTP Binding	Select the HTTP binding associated with the **Identity Provider SLO URL**. The firewall uses the binding to send SAML messages to the IdP. The options are:

SAML Identity Provider Server Settings	Description
	• **POST**—The firewall sends messages using base64-encoded HTML forms. • **Redirect**—The firewall sends base64-encoded and URL-encoded SSO messages within URL parameters. *If you import an IdP metadata file that has multiple SLO URLs, the firewall uses the binding of the first URL that uses the POST or redirect method. The firewall ignores URLs that use other bindings.*
Identity Provider Metadata	This field displays only if you **Import** an IdP metadata file that you uploaded to the firewall from the IdP. The file specifies the values and signing certificate for a new SAML IdP server profile. **Browse** to the file, specify the Profile Name and Maximum Clock Skew, and then click **OK** to create the profile. Optionally, you can edit the profile to change the imported values.
Validate Identity Provider Certificate	Select this option to validate the chain of trust and optionally the revocation status of the IdP signing certificate. To enable this option, a Certificate Authority (CA) must issue your IdP's signing certificate. You must create a Certificate Profile that has the CA that issued the IdP's signing certificate. In the Authentication Profile, select the SAML Server profile and Certificate Profile to validate the IdP certificate (see Device > Authentication Profile). If your IdP signing certificate is a self-signed certificate, there is no chain of trust; as a result, you cannot enable this option. The firewall always validates the signature of the SAML Responses or Assertions against the Identity Provider certificate that you configure whether or not you enable the **Validate Identity Provider Certificate** option. If your IdP provides a self-signed certificate, ensure that you are using PAN-OS 10.0 to mitigate exposure to CVE-2020-2021.
Sign SAML Message to IdP	Select this option to specify that the firewall sign messages it sends to the IdP. The firewall uses the **Certificate for Signing Requests** that you specify in an authentication profile (see Device > Authentication Profile). *Using a signing certificate ensures the integrity of messages sent to the IdP.*
Maximum Clock Skew	Enter the maximum acceptable time difference in seconds between the IdP and firewall system times at the moment when the firewall validates a message that it receives from the IdP (range is 1 to 900; default is 60). If the time difference exceeds this value, the validation (and thus authentication) fails.

Device > Server Profiles > DNS

To simplify configuration for a virtual system, a DNS server profile allows you to specify the virtual system that is being configured, an inheritance source or the primary and secondary DNS addresses for DNS servers, and the source interface and source address (service route) that will be used in packets sent to the DNS server. The source interface and source address are used as the destination interface and destination address in the reply from the DNS server.

A DNS server profile is for a virtual system only; it is not for the global Shared location.

DNS Server Profile Settings	Description
Name	Name the DNS Server profile.
Location	Select the virtual system to which the profile applies.
Inheritance Source	Select **None** if the DNS server addresses are not inherited. Otherwise, specify the DNS server from which the profile should inherit settings.
Check inheritance source status	Click to see the inheritance source information.
Primary DNS	Specify the IP address of the primary DNS server.
Secondary DNS	Specify the IP address of the secondary DNS server.
Service Route IPv4	Select this option if you want to specify that packets going to the DNS server are sourced from an IPv4 address.
Source Interface	Specify the source interface that packets going to the DNS server will use.
Source Address	Specify the IPv4 source address from which packets going to the DNS server are sourced.
Service Route IPv6	Select this option if you want to specify that packets going to the DNS server are sourced from an IPv6 address.
Source Interface	Specify the source interface that packets going to the DNS server will use.
Source Address	Specify the IPv6 source address from which packets going to the DNS server are sourced.

Device > Server Profiles > Multi Factor Authentication

Use this page to configure a multi-factor authentication (MFA) server profile that defines how the firewall connects to an MFA server. MFA can protect your most sensitive resources by ensuring that attackers cannot access your network and move laterally through it by compromising a single authentication factor (for example, stealing login credentials). After configuring the server profile, assign it to authentication profiles for the services that require authentication (see Device > Authentication Profile).

For the following authentication use cases, the firewall integrates with multi-factor authentication (MFA) vendors using RADIUS and SAML:

- Remote user authentication through GlobalProtect™ portals and gateways.
- Administrator authentication in the PAN-OS and Panorama™ web interface.
- Authentication through Authentication policy.

Additionally, the firewall can also integrate with MFA vendors using the API to enforce MFA through Authentication policy for end-user authentication only (not for GlobalProtect authentication or administrator authentication).

The complete procedure to configure MFA requires additional tasks besides creating a server profile.

Authentication sequences do not support authentication profiles that specify MFA server profiles.

If the firewall integrates with your MFA vendor through RADIUS, configure a RADIUS server profile (see Device > Server Profiles > RADIUS). The firewall supports all MFA vendors through RADIUS.

MFA Server Settings	Description
Profile Name	Enter a name to identify the server (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	On a firewall that has more than one virtual system (vsys), select a vsys or the **Shared** location. After you save the profile, you cannot change its **Location**.
Certificate Profile	Select the **Certificate Profile** that specifies the certificate authority (CA) certificate that the firewall will use to validate the MFA server certificate when setting up a secure connection to the server. For details, see Device > Certificate Management > Certificate Profile.
MFA Vendor / Value	Select an MFA vendor **MFA Vendor** and enter a **Value** for each vendor attribute. The attributes vary by vendor. Refer to your vendor documentation for the correct values. • **Duo v2**: • **API Host**—The hostname of the Duo v2 server. • **Integration Key** and **Secret Key**—The firewall uses these keys to authenticate to the Duo v2 server and to sign authentication requests

MFA Server Settings	Description
	that it sends to the server. To secure these keys, the master key on the firewall automatically encrypts them so that their plaintext values are not exposed anywhere in the firewall storage. Contact your Duo v2 administrator to obtain the keys. • **Timeout**—Enter the time in seconds after which the firewall times out when attempting to communicate with the **API Host** (range is 5 to 600; default is 30). This interval must be longer than the timeout between the API host and the endpoint device of the user. • **Base URI**—If your organization hosts a local authentication proxy server for the Duo v2 server, enter the proxy server URI (default /auth/v2). • **Okta Adaptive**: • **API Host**—The hostname of the Okta server. • **Base URI**—If your organization hosts a local authentication proxy server for the Okta server, enter the proxy server URI (default /api/v1). • **Token**—The firewall uses this token to authenticate to the Okta server and to sign authentication requests that it sends to the server. To secure the token, the master key on the firewall automatically encrypts it so that its plaintext value is not exposed anywhere in the firewall storage. Contact your Okta administrator to obtain the token. • **Organization**—The subdomain for your organization in the **API Host**. • **Timeout**—Enter the time in seconds after which the firewall times out when attempting to communicate with the **API Host** (range is 5 to 600; default is 30). This interval must be longer than the timeout between the API host and the endpoint device of the user. • **PingID**: • **Base URI**—If your organization hosts a local authentication proxy server for the PingID server, enter the proxy server URI (default /pingid/rest/4). • **Host name**—Enter the host name of the PingID server (default idpxnyl3m.pingidentity.com). • **Use Base64 Key** and **Token**—The firewall uses the key and token to authenticate to the PingID server and to sign authentication requests that it sends to the server. To secure the key and token, the master key on the firewall automatically encrypts them so that their plaintext values are not exposed anywhere in the firewall storage. Contact your PingID administrator to obtain the values. • **PingID Client Organization ID**—The PingID identifier for your organization. • **Timeout**—Enter the time in seconds after which the firewall times out when attempting to communicate with the PingID server specified in the **Host name** field (range is 5 to 600; default is 30). This interval must be longer than the timeout between the PingID server and the endpoint device of the user.

Device > Local User Database > Users

You can set up a local database on the firewall to store authentication information for firewall administrators, Authentication Portal end users, and end users who authenticate to a GlobalProtect portal and GlobalProtect gateway. Local database authentication requires no external authentication service; you perform all account management on the firewall. After creating the local database and (optionally) assigning the users to groups (see Device > Local User Database > User Groups), you can Device > Authentication Profile based on the local database.

You cannot configure Device > Password Profiles *for administrative accounts that use local database authentication.*

To **Add** a local user to the database, configure the settings described in the following table.

Local User Settings	Description
Name	Enter a name to identify the user (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the user account is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the user account, you can't change its **Location**.
Mode	Use this field to specify the authentication option: • **Password**—Enter and confirm a password for the user. • **Password Hash**—Enter a hashed password string. This can be useful if, for example, you want to reuse the credentials for an existing Unix account but don't know the plaintext password, only the hashed password. The firewall accepts any string of up to 63 characters regardless of the algorithm used to generate the hash value. The operational CLI command **`request password-hash password`** uses the MD5 algorithm when the firewall is in normal mode and the SHA256 algorithm when the firewall is in CC/FIPS mode. *Any* Minimum Password Complexity *parameters you set for the firewall (Device > Setup > Management) do not apply to accounts that use a Password Hash.*
Enable	Select this option to activate the user account.

Device > Local User Database > User Groups

Select **Device** > **Local User Database** > **User Groups** to add user group information to the local database.

Local User Group Settings	Description
Name	Enter a name to identify the group (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the user group is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select **Shared** (all virtual systems). In any other context, you can't select the **Location**; its value is predefined as Shared (firewalls) or as Panorama. After you save the user group, you can't change its **Location**.
All Local Users	Click **Add** to select the users you want to add to the group.

Device > Scheduled Log Export

You can schedule exports of logs and save them in CSV format to a File Transfer Protocol (FTP) server or use Secure Copy (SCP) to securely transfer data between the firewall and a remote host. Log profiles contain the schedule and FTP server information. For example, a profile may specify that the previous day's logs are collected each day at 3AM and stored on a particular FTP server.

Click **Add** and fill in the following details:

Scheduled Log Export Settings	Description
Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. You cannot change the name after the profile is created.
Description	Enter an optional description (up to 255 characters).
Enable	Select this option to enable the scheduling of log exports.
Log Type	Select the type of log (**traffic**, **threat**, **gtp**, **sctp**, **tunnel**, **userid**, **auth**, **url**, **data**, **hipmatch**, or **wildfire**). Default is traffic.
Scheduled Export Start Time (Daily)	Enter the time of day (hh:mm) to start the export using a 24-hour clock (00:00 - 23:59).
Protocol	Select the protocol to use to export logs from the firewall to a remote host: • **FTP**—This protocol is not secure. • **SCP**—This protocol is secure. After completing the remaining fields, you must click **Test SCP server connection** to test connectivity between the firewall and the SCP server and you must verify and accept the host key of the SCP server.
Hostname	Enter the host name or IP address of the FTP server that will be used for the export.
Port	Enter the port number that the FTP server will use. Default is 21.
Path	Specify the path located on the FTP server that will be used to store the exported information.
Enable FTP Passive Mode	Select this option to use passive mode for the export. By default, this option is selected.
Username	Enter the user name for access to the FTP server. Default is anonymous.
Password / Confirm Password	Enter the password for access to the FTP server. A password is not required if the user is anonymous.

Scheduled Log Export Settings	Description
Test SCP server connection (SCP protocol only)	If you set the **Protocol** to **SCP**, you must click this button to test connectivity between the firewall and the SCP server and then verify and accept the host key of the SCP server. *If you use a Panorama template to configure the log export schedule, you must perform this step after committing the template configuration to the firewalls. After the template commit, log in to each firewall, open the log export schedule, and click Test SCP server connection.*

Device > Software

Select **Device** > **Software** to view the available software releases, to download or upload a release, to install a release (a support license is required), to delete a software image from the firewall, or to view release notes.

Before you upgrade or downgrading your software version:

- Review the current Release Notes to view descriptions of new features and changes to default behaviors in a release and to view the migration path to upgrade software.
- Review the upgrade and downgrade considerations and upgrade instructions in the PAN-OS® 10.0 New Features Guide.
- Ensure that the date and time settings on the firewall are current. PAN-OS software is digitally signed and the firewall checks the signature before installing a new version. If the date and time settings on the firewall are not current and the firewall perceives that the software signature is (erroneously) in the future, it will display the following message:

```
Decrypt failed: GnuPG edit non-zero, with code 171072 Failed to load into
 PAN software manager.
```

The following table provides help for using the **Software** page.

Software Options Fields	Description
Version	Lists the software versions that are currently available on the Palo Alto Networks Update Server. To check if a new software release is available from Palo Alto Networks, click **Check Now**. The firewall uses the service route to connect to the Update Server and checks for new versions and, if there are updates available, and displays them at the top of the list.
Size	Indicates the size of the software image.
Release Date	Indicates the date and time Palo Alto Networks made the release available.
Available	Indicates that the corresponding version of the software image is uploaded or downloaded to the firewall.
Currently Installed	Indicates whether the corresponding version of the software image is activated and is currently running on the firewall.
Action	Indicates the current action you can take for the corresponding software image as follows: • **Download**—The corresponding software version is available on the Palo Alto Networks Update Server; click to **Download** an available software version. • **Install**—The corresponding software version has been downloaded or uploaded to the firewall; click to **Install** the software. A reboot is required to complete the upgrade process. • **Reinstall**—The corresponding software version was installed previously; click to **Reinstall** the same version.

Software Options Fields	Description
Release Notes	Provides a link to the release notes for the corresponding software update. This link is only available for updates that you download from the Palo Alto Networks Update Server: it is not available for uploaded updates.
	Removes the previously downloaded or uploaded software image from the firewall. You would only want to delete the base image for older releases that will not need upgrading. For example, if you are running 7.0, you can remove the base image for 6.1 unless you think you might need to downgrade.
Check Now	Checks whether a new software update is available from Palo Alto Networks.
Upload	Imports a software update image from a computer that the firewall can access. Typically, you perform this action if the firewall doesn't have Internet access, which is required when downloading updates from the Palo Alto Networks Update Server. For uploads, use an Internet-connected computer to visit the Palo Alto Networks website, download the software image from the Support site (Software Updates), download the update to your computer, select **Device** > **Software** on the firewall and **Upload** the software image. In a high availability (HA) configuration, you can select **Sync To Peer** to push the imported software image to the HA peer. After the upload, the **Software** page displays the same information (for example, version and size) and **Install**/**Reinstall** options for uploaded and downloaded software. **Release Notes** option is not active for uploaded software.

Device > Dynamic Updates

- Device > Dynamic Updates
- Panorama > Dynamic Updates

Palo Alto Networks regularly posts updates that include new and modified applications, threat protection, and GlobalProtect data files through dynamic updates. The firewall can retrieve these updates and use them to enforce policy, without requiring configuration changes. Application and some antivirus updates are available without a subscription; other are tied to your subscriptions.

You can view the latest updates, read the release notes for each update, and then select the update you want to download and install. You can also revert to a previously installed version of an update.

Setting a schedule for dynamic updates allows you to define the frequency at which the firewall checks for and downloads or installs new updates. Particularly for Applications and Threats content updates, you might want to set a schedule that staggers new and modified application updates behind threat updates; this gives you more time to assess how new and modified applications impact your security policy, while ensuring that the firewall is always equipped with the latest threat protections.

Dynamic Updates Options	Description
Version	Lists the versions that are currently available on the Palo Alto Networks Update Server. To check if a new software release is available from Palo Alto Networks, click **Check Now**. The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list.
Last checked	Displays the date and time that the firewall last connected to the update server and checked if an update was available.
Schedule	Allows you to schedule the frequency for retrieving updates. You can define how often and when the dynamic content updates occur—the **Recurrence** and time—and whether to **Download Only** or to **Download and Install** scheduled updates For Antivirus and Applications and Threats updates, you have the option to set a minimum Threshold of time that a content update must be available before the firewall installs it. Very rarely, there can be an error in a content update and this threshold ensures that the firewall only downloads content releases that have been available and functioning in customer environments for the specified amount of time. For Applications and Threats content updates, you can also set a threshold that applies specifically to content updates with new and modified applications. An extended application threshold gives you more time to assess and adjust your security policy based on changes that new or modified applications introduce. For WildFire updates, you have the option to retrieve signatures in real-time, allowing you to access the signatures as soon as they are generated. Signatures that are downloaded during a sample check are saved in the firewall cache, and are available for fast (local) look-ups. In addition, to maximize coverage, the firewall also automatically downloads an

Dynamic Updates Options	Description
	additional signature package on a regular basis when real-time signatures is enabled. These supplemental signatures are added to the firewall cache and remain available until they become stale and are refreshed or are overwritten by new signatures. *For guidance on how to best enable Application and Threat content updates to achieve both constant application availability and the latest threat protection, review the* Best Practices for Application and Threat Updates
File Name	List the filename; it includes the content version information.
Features	Lists what type of signatures the content version might include. For Applications and Threats content release versions, this field might display an option to review **Apps, Threats**. Click this option to view new application signatures made available since the last content release version installed on the firewall. You can also use the **New Applications** dialog to **Enable/Disable** new applications. You might choose to disable a new application included in a content release if you want to avoid any policy impact from an application being uniquely identified (an application might be treated differently before and after a content installation if a previously unknown application is identified and categorized differently).
Type	Indicates whether the download includes a full database update or an incremental update.
Size	Displays the size of the content update package.
Release Date	The date and time Palo Alto Networks made the content release available.
Downloaded	A check mark in this column indicates that the corresponding content release version has been downloaded to the firewall.
Currently Installed	A check mark in this column indicates that the corresponding content release version is currently running on the firewall.
Action	Indicates the current action you can take for the corresponding software image as follows: • **Download**—The corresponding content release version is available on the Palo Alto Networks Update Server; click to **Download** the content release version. If the firewall does not have access to the Internet, use an Internet-connected computer to go to the Customer Support Portal and select **Dynamic Updates**. Find the content release version you want and click **Download** to save the update package to your local computer. Then manually **Upload** the software image to the firewall. Additionally, downloading an Application and Threat content release version enables the option to **Review Policies** that are affected by new application signatures included with the release.

Dynamic Updates Options	Description
	• **Review Policies** (Application and Threat content only)—Review any policy impact for new applications included in a content release version. Use this option to assess the treatment an application receives both before and after installing a content update. You can also use the Policy Review dialog to add or remove a pending application (an application that is downloaded with a content release version but is not installed on the firewall) to or from an existing Security policy rule; policy changes for pending applications do not take effect until the corresponding content release version is installed. • **Review Apps** (Application and Threat content only)—View new and modified application signatures made available since the last content release version installed on the firewall. In cases where a content update introduces changes that might impact the enforcement of critical applications, those applications are marked as recommended for policy review. Click on Review Policies to see how content updates impact your existing security policy or, you can disable an application until you have time to review the application's policy impact. • **Install**—The corresponding content release version has been downloaded to the firewall; click to **Install** the update. When installing a new Applications and Threats content release version, you are prompted with the option to **Disable new apps in content update**. This option enables protection against the latest threats, while giving you the flexibility to enable applications after preparing any policy updates, due to the impact of new application signatures (to enable applications you have previously disabled, select **Apps, Threats** on the Dynamic Updates page or select **Objects** > **Applications**). • **Revert**—The corresponding content release version has been downloaded previously To reinstall the same version, click **Revert**.
Documentation	Provides a link to the release notes for the corresponding version.
	Remove the previously downloaded content release version from the firewall.
Upload	If the firewall does not have access to the Palo Alto Networks Update Server, you can manually download dynamic updates from the Palo Alto Networks Support site in the Dynamic Updates section. After you download an update to your computer, **Upload** the update to the firewall. You then select **Install From File** and select the file you downloaded.
Install From File	After you manually upload an update file to the firewall, use this option to install the file. In the **Package Type** drop-down, select the type of update you are installing (**Application and Threats**, **Antivirus**, or **WildFire**), click **OK**, select the file you want to install and then click **OK** again to start the installation.

Device > Licenses

Select **Device** > **Licenses** to activate licenses on all firewall models. When you purchase a subscription from Palo Alto Networks, you receive an authorization code to activate one or more license keys.

On the VM-Series firewall, this page also allows you to deactivate a virtual machine (VM).

The following actions are available on the Licenses page:

- Retrieve license keys from license server: Select to enable purchased subscriptions that require an authorization code and have been activated on the support portal.
- Activate feature using authorization code: Select to enable purchased subscriptions that require an authorization code and have not been previously activated on the support portal. Then enter your authorization code, and click **OK**.
- Manually upload license key: If the firewall does not have connectivity to the license server and you want to upload license keys manually, download the license key file from https://support.paloaltonetworks.com, and save it locally. Click Manually upload license key, click Browse, select the file, and then click OK.

  To enable licenses for URL filtering, you must install the license, download the database, and click Activate. If you are using PAN-DB for URL Filtering, you will need to Download the initial seed database first and then Activate.

  You can also run the CLI command ***`request url-filtering download paloaltonetworks region < regionname>`***.
- **Deactivate VM**: This option is available on the VM-Series firewall with the Bring Your Own License model that supports perpetual and term-based licenses; the on-demand license model does not support this functionality. Click **Deactivate VM** when you no longer need an instance of the VM-Series firewall. It allows you to free up all active licenses—subscription licenses, VM-Capacity licenses, and support entitlements— using this option. The licenses are credited back to your account and you can then apply the licenses on a new instance of a VM-Series firewall, when you need it. When the license is deactivated, the VM-Series firewall functionality is disabled and the firewall is in an unlicensed state. However, the configuration remains intact.
  - Click **Continue Manually** if the VM-Series firewall does not have direct internet access. The firewall generates a token file. Click **Export license token** to save the token file to your local computer and then reboot the firewall. Log in to the Palo Alto Networks Support portal, select **Assets** > **Devices**, and **Deactivate VM** to use this token file and complete the deactivation process.
  - Click **Continue** to deactivate the licenses on the VM-Series firewall. Click **Reboot Now** to complete the license deactivation process.
  - Click **Cancel** if you want to cancel and close the Deactivate VM window.
- **Upgrade VM Capacity**: This option allows you to upgrade the capacity of your currently licensed VM-Series firewall. Upon upgrading the capacity, the VM-Series firewall retains all configuration and subscriptions it had prior to the upgrade.
  - If your firewall has connectivity to the license server—Select **Authorization Code**, enter your authorization code in the Authorization Code field, and click **Continue** to initiate the capacity upgrade.
  - If your firewall does not have connectivity to the license server—Select **License Key**, click **Complete Manually** to generate a token file, and save the token file to your local computer. Then log in to the Palo Alto Networks Support portal, select **Assets** > **Devices**, and **Deactivate License(s)** to use the token file. Download the license key for your VM-Series firewall to your local computer, add the license key to the firewall, and click **Continue** to complete the capacity upgrade.
  - If your firewall has connectivity to the license server but you do not have an Authorization Code—Select **Fetch from license server**, upgrade the firewall's capacity license on the license server before

you attempt to upgrade the capacity, and then after you verify that the license is upgraded on the license server, click **Continue** to initiate the capacity upgrade.

Device > Support

- Device > Support
- Panorama > Support

Select **Device** > **Support** or **Panorama** > **Support** to access support related options. You can view the Palo Alto Networks contact information, view your support expiration date, and view product and security alerts from Palo Alto Networks based on the serial number of your firewall.

Perform any of the following functions on this page:

- **Support**—Provides information on the support status of the device and provides a link to activate support using an authorization code.
- **Production Alerts/Application and Threat Alerts**—These alerts will be retrieved from the Palo Alto Networks update servers when this page is accessed/refreshed. To view the details of production alerts, or application and threat alerts, click the alert name. Production alerts will be posted if there is a large scale recall or urgent issue related to a given release. The application and threat alerts will be posted if significant threats are discovered.
- **Links**—Provides common support links to help you manage your device and to access support contact information.
- **Tech Support File**—Click **Generate Tech Support File** to generate a system file that the support team can use to help troubleshoot issues that you may be experiencing with the firewall. After you generate the file, **Download Tech Support File** and then send it to the Palo Alto Networks Support department.

  If your browser is configured to automatically open files after download, you should turn off that option so the browser downloads the support file instead of attempting to open and extract it.
- **Stats Dump File** (firewall only)—Click **Generate Stats Dump File** to generate a set of XML reports that summarizes network traffic over the last 7 days. After the report is generated, you can **Download Stats Dump File**. The Palo Alto Networks or Authorized Partner systems engineer uses the report to generate a Security Lifecycle Review (SLR). The SLR highlights what has been found on the network and the associated business or security risks that may be present and is typically used as part of the evaluation process. For more information on the SLR, contact your Palo Alto Networks or Authorized Partner systems engineer.
- **Core Files**—If your firewall experiences a system process failure it will generate a core file that contains details about the process and why it failed. Click the **Download Core Files** link to view a list of available core files and then click a core file name to download it. After you download the file, upload it to a Palo Alto Networks support case to obtain assistance in resolving the issue.

  The contents of the core files can be interpreted only by a Palo Alto Networks support engineer.

Device > Master Key and Diagnostics

- **Device** > **Master Key and Diagnostics**
- **Panorama** > **Master Key and Diagnostics**

Edit the master key that encrypts all passwords and private keys on the firewall or Panorama (such as the RSA key for authenticating administrators who access the CLI). Encrypting passwords and keys improves security by ensuring their plaintext values are not exposed anywhere on the firewall or Panorama.

The only way to restore the default master key is to perform a factory reset.

Palo Alto Networks recommends you configure a new master key instead of using the default key, store the key in a safe location, and periodically change it. For extra privacy, you can use a hardware security module to encrypt the master key (see Device > Setup > HSM). Configuring a unique master key on each firewall or Panorama management server ensures that an attacker who learns the master key for one appliance cannot access the passwords and private keys on any of your other appliances. However, you must use the same master key across multiple appliances in the following cases:

- **High availability (HA) configurations**—If you deploy firewalls or Panorama in an HA configuration, use the same master key on both firewalls or Panorama management servers in the pair. Otherwise, HA synchronization does not work.
- **Panorama pushes configurations to firewalls**—If you use Panorama to push configurations to managed firewalls, use the same master key on Panorama and the managed firewalls. Otherwise, push operations from Panorama will fail.

To configure a master key, edit the Master Key settings and use the following table to determine the appropriate values:

Master Key and Diagnostics Settings	Description
Master Key	Enable to configure a unique master key. Disable (clear) to use the default master key.
Current Master Key	Specify the key that is currently used to encrypt all of the private keys and passwords on the firewall.
New Master Key Confirm Master Key	To change the master key, enter a 16-character string and confirm the new key.
Life Time	Specify the number of **Days** and **Hours** after which the master key expires. Range is 1 to 438,000 days (50 years). You must configure a new master key before the current key expires. If the master key expires, the firewall or Panorama automatically reboots in Maintenance mode. You must then perform a factory reset.  *Set the Lifetime to two years or less, depending on how many encryptions the device performs. The more encryptions a device performs, the short the Lifetime you should set. The critical consideration is to not run out of unique encryptions before you change the master*

Master Key and Diagnostics Settings	Description
	key. Each master key can provide up to 2^^32 unique encryptions and then encryptions repeat, which is a security risk. *Set a Time for Reminder for the master key and when the reminder notification occurs, change the master key.*
Time for Reminder	Enter the number of **Days** and **Hours** before the master key expires when the firewall generates an expiration alarm. The firewall automatically opens the System Alarms dialog to display the alarm.  *Set the reminder so that it gives you plenty of time to configure a new master key before it expires in a scheduled maintenance window. When the Time for Reminder expires and the firewall or Panorama sends a notification log, change the master key, don't wait for the Lifetime to expire. For grouped devices, track every device (e.g., firewalls that Panorama manages and firewall HA pairs) and when the reminder value expires for the any device in the group, change the master key.* *To ensure the expiration alarm displays, select Device > Log Settings, edit the Alarm Settings, and Enable Alarms.*
Stored on HSM	Enable this option only if the master key is encrypted on a Hardware Security Module (HSM). You cannot use HSM on a dynamic interface such as a DHCP client or PPPoE. The HSM configuration is not synchronized between peer firewalls in HA mode. Therefore, each peer in an HA pair can connect to a different HSM source. If you are using Panorama and need to keep both peer configurations in sync, use Panorama templates to configure the HSM source on the managed firewalls. The PA-220 does not support HSM.
Auto Renew Master Key	Enable to automatically renew the master key for a specified number of days and hours. Disable (clear) to allow the master key to expire after the configured key life time. **Auto Renew with Same Master Key** by specifying the number of **Days** and **Hours** by which to extend the master key encryption (range is 1 hour to 730 days).  *If you enable Auto Renew Master Key, set it so that the total time (lifetime plus the auto renew time) does not cause the device to run out of unique encryptions. For example, if you believe the device will consume the master key's number of unique encryptions in two and a half years, you could set the Lifetime for two years, set the Time for Reminder to 60 days, and set the Auto Renew Master Key for 60-90 days to provide the extra time to configure a new master key before the Lifetime expires. However, the best*

Master Key and Diagnostics Settings	Description
	practice is still to change the master key before the lifetime expires to ensure that no device repeats encryptions.
Common Criteria	In Common Criteria mode, additional options are available to run a cryptographic algorithm self-test and software integrity self-test. A scheduler is also included to specify the times at which the two self-tests will run.

Deploy Master Key

Deploy a master key or update an existing master key of a managed firewall, Log Collector, or WF-500 appliance directly from Panorama.

Field	Description
Deploy Master Key	
Filter	Filter for which managed devices to display based on Platform, Device Groups, Templates, Tags, HA Status, or Software Version.
Device Name	Name of the managed firewall.
Software Version	Software version running on the managed device.
Status	Connection status of the managed device: can `Connected`, `Disconnected`, or `Unknown`.
Deploy Master Key Job Status	
Device Name	Name of the managed firewall.
Status	Status of the master key deployment job.
Result	Results of the master key deployment job. Can be `OK` or `FAIL`.
Progress	Progress (%) of the master key deployment job.
Details	Details about the master key deployment job. If the job failed, details describing the reasons for failing are displayed here.
Summary	
Progress	Displays a progress bar indicating the progress of the master key deployment job. the following information is displayed: • **Results Succeeded**—Number of devices the master key was successfully deployed to.

Field	Description
	• **Results Pending**—Number of devices for which the master key deployment job is currently pending. • **Results Failed**—Number of devices for which the master key deployment job failed.

Device > Policy Recommendation

View information on the policy rule recommendations from the IoT Security app. The policy rule recommendation uses metadata that the firewall collects from traffic on your network to determine what behavior to allow for the device. You can check the policy rule recommendation version in **Device** > **Dynamic Updates** > **Device-ID Content**.

Button/Field	Description
Policy Import Details	View detailed information about the policy rule recommendation, such as device group **Location**, **rule name**, the **user** who imported the policy, whether the policy rule recommendation **Is Updated**, when the policy rule recommendation was imported, and when the policy rule recommendation was last updated.
Device Profile	The device profile for the source device in the policy rule recommendation.
Source Zones	The source zones for the policy rule recommendation.
Address	The source address for the policy rule recommendation.
Location	The device group on Panorama where this policy rule recommendation is available.
Destination Device Profile	The destination device profile that the firewall allows for the policy rule recommendation.
Device IP	The IP address of the device that the policy rule recommendation allows.
FQDN	The fully qualified domain name (FQDN) that the policy rule recommendation identifies as allowed based on typical behavior for the device.
Destination Zones	The destination zones that the policy rule recommendation allows.
Security Profiles	The security profile that the policy rule recommendation allows.
Services	The services (for example, ssl) that the policy rule recommendation allows.
URL Category	The URL filtering categories that the policy rule recommendation allows.

Button/Field	Description
Applications	The applications that the policy rule recommendation allows.
Tags	The tags that identify the policy rule for the policy rule recommendation. *Do not change the tags of the policy rule; if you change the tags, the firewall cannot rebuild the policy mappings.*
Internal Device	Identifies whether the device is from a zone that is internal to your network (`Yes`) or from an external internet-facing zone (`No`).
Active Recommendation	Identifies whether this policy rule recommendation is `active` and currently used in security policy or whether you have `removed` it from your security policy.
Action	Identifies the action for this policy rule recommendation (default is `allow`).
New Update Available	Identifies that there is a new update for this policy rule recommendation that you must import from the IoT Security app. When you import the policy rule recommendation update, the firewall dynamically updates the security policy rule. If you have more than one device group, the value remains `Yes` until you import the policy rule recommendation update to all device groups.
Import Policy	After using the IoT Security app to **Activate** your policy rule recommendations, **Import Policy** to import the policy rule recommendations to use in your security policy rules.
Remove Policy Mapping	If you no longer need the policy rule recommendation for a device, you can **Remove Policy Mapping** for it. *You must also delete the policy rule for the policy rule recommendation.*
Rebuild All Mappings	If the mappings become out of sync (for example, if you restore a previous configuration) you can **Rebuild All Mappings** to restore the policy rule recommendation mappings.

User Identification

User Identification (User-ID™) is a Palo Alto Networks® next-generation firewall feature that seamlessly integrates with a range of enterprise directory and terminal services to tie application activity and policies to usernames and groups instead of just IP addresses. Configuring User-ID enables the Application Command Center (ACC), App Scope, reports, and logs to include usernames in addition to user IP addresses.

- Device > User Identification > User Mapping
- Device > User Identification > Connection Security
- Device > User Identification > Terminal Server Agents
- Device > User Identification > Group Mapping Settings
- Device > User Identification > Authentication Portal Settings

Looking for more?

See User-ID

Device > User Identification > User Mapping

Configure the PAN-OS integrated User-ID agent that runs on the firewall to map IP addresses to usernames.

What are you looking for?	See:
Configure the PAN-OS integrated User-ID agent.	Palo Alto Networks User-ID Agent Setup
Manage access to the servers that the User-ID agent monitors for user mapping information.	Monitor Servers
Manage the subnetworks that the firewall includes or excludes when mapping IP addresses to usernames.	Include or Exclude Subnetworks for User Mapping
Looking for more?	Configure User Mapping Using the PAN-OS IntegratedUser-IDAgent.

Palo Alto Networks User-ID Agent Setup

These settings define the methods that the User-ID agent uses to perform user mapping.

What are you looking for?	See:
Enable the User-ID agent to use Windows Management Instrumentation (WMI) to probe client systems or Windows Remote Management (WinRM) over HTTP or HTTPS to monitor servers for user mapping information.	Server Monitor Account
Monitor server logs for user mapping information with the User-ID agent.	Server Monitoring
Enable the User-ID agent to probe client systems for user mapping information.	Client Probing
Ensure that the firewall has the most current user mapping information as users roam and obtain new IP addresses.	Cache

What are you looking for?	See:
Configure the User-ID agent to parse syslog messages for user mapping information.	Syslog Filters
Configure the User-ID agent to omit specific usernames from the mapping process.	Ignore User List

Server Monitor Account

- **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Server Monitor Account**

To configure the PAN-OS integrated User-ID agent to use Windows Management Instrumentation (WMI) for probing client systems or Windows Remote Management (WinRM) over HTTP or over HTTPS to monitor servers for user mapping information, complete the following fields.

You can also Configure Access to Monitored Servers by configuring a Kerberos server to authenticate server monitoring using Windows Remote Management (WinRM) over HTTP or over HTTPS.

Because WMI probing trusts data that is reported back from an endpoint, Palo Alto Network recommends that you do not use this method to obtain User-ID mapping information in a high-security network. If you configure the User-ID agent to obtain mapping information by parsing Active Directory (AD) security event logs or syslog messages, or using the XML API, Palo Alto Networks recommends you disable WMI probing.

If you do use WMI probing, do not enable it on external, untrusted interfaces. Doing so causes the agent to send WMI probes containing sensitive information—such as the username, domain name, and password hash of the User-ID agent service account—outside of your network. An attacker could potentially exploit this information to penetrate and gain further access to your network.

Active Directory Authentication Settings	Description
User Name	Enter the domain credentials (**User Name** and **Password**) for the account that the firewall will use to access Windows resources. The account requires permissions to perform WMI queries on client computers and to monitor Microsoft Exchange servers and domain controllers. Use domain\username syntax for the **User Name**. If you Configure Access to Monitored Servers using Kerberos for server authentication, enter the Kerberos User Principal Name (UPN).
Domain's DNS Name	Enter the DNS name of the monitored server. If you Configure Access to Monitored Servers using Kerberos for server authentication, enter the Kerberos Realm domain. You must configure this setting if you are using **WinRM-HTTP** as the transport protocol when you Configure Access to Monitored Servers.
Password/Confirm Password	Enter and confirm the password for the account that the firewall uses to access Windows resources.
Kerberos Server Profile	Select the Kerberos Server Profile for the Kerberos server that controls access to the Realm to retrieve security logs and session

Active Directory Authentication Settings	Description
	information from the monitored server with WinRM over HTTP or over HTTPS.

The complete procedure to configure the PAN-OS integrated User-ID agent to monitor servers and probe clients requires additional tasks besides defining the Active Directory authentication settings.

Server Monitoring

- **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Server Monitor**

To enable the User-ID agent to map IP addresses to usernames by searching for logon events in the security event logs of servers, configure the settings described in the following table.

If the query load is high for Windows server logs, Windows server sessions, or eDirectory servers, the observed delay between queries might significantly exceed the specified frequency or interval.

The complete procedure to configure the PAN-OS integrated User-ID agent to monitor servers requires additional tasks besides configuring the server monitoring settings.

Server Monitoring Settings	Description
Enable Security Log	Select this option to enable security log monitoring on Windows servers.
Server Log Monitor Frequency (sec)	Specify the frequency in seconds at which the firewall will query Windows server security logs for user mapping information (range is 1-3600; default is 2). This is the interval between when the firewall finishes processing the last query and when the firewall sends the next query. *If the log monitoring doesn't happen often enough, the latest IP-address-to-user mapping may not be available. If the firewall monitors logs too frequently, that may impact the domain controller, memory, CPU, and User-ID policy enforcement. Start with a value in a range of 2-30 seconds, then revise the value based on performance impact or how often user mappings are updated.*
Enable Session	Select this option to enable monitoring of user sessions on the monitored servers. Each time a user connects to a server, a session is created; the firewall can use this information to identify the user IP address. *Do not Enable Session. This setting requires that the User-ID agent have an Active Directory account with Server Operator privileges so that it can read all user*

Server Monitoring Settings	Description
	sessions. Instead, you should use a Syslog or XML API integration to monitor sources that capture login and logout events for all device types and operating systems (instead of only Windows operating systems), such as wireless controllers and NACs.
Server Session Read Frequency (sec)	Specify the frequency in seconds at which the firewall will query Windows server user sessions for user mapping information (range is 1-3600; default is 10). This is the interval between when the firewall finishes processing the last query and when it starts the next query.
Novell eDirectory Query Interval (sec)	Specify the frequency in seconds at which the firewall will query Novell eDirectory servers for user mapping information (range is 1-3600; default is 30). This is the interval between when the firewall finishes processing the last query and when it starts the next query.
Syslog Service Profile	Select an SSL/TLS service profile that specifies the certificate and allowed SSL/TLS versions for communications between the firewall and any syslog senders that the User-ID agent monitors. For details, see Device > Certificate Management > SSL/TLS Service Profile and Syslog Filters. If you select **none**, the firewall uses its predefined, self-signed certificate.

Client Probing

- **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Client Probing**

You can configure the User-ID agent to perform WMI client probing for each client system that the user mapping process identifies. The User-ID agent will periodically probe each learned IP address to verify that the same user is still logged in. When the firewall encounters an IP address for which it has no user mapping, it sends the address to the User-ID agent for an immediate probe. To configure client probing settings, complete the following fields.

Do not enable client probing on high-security networks. Do not enable client probing on external untrusted interfaces. Client probing can generate a large amount of network traffic, can pose a security threat when misconfigured, and if enabled on an external untrusted zone, client probing could allow an attacker to send a probe outside of your network and result in disclosure of the User-ID agent service account name, domain name, and encrypted password hash. Instead, collect user mapping information from more isolated and trusted sources, such as domain controllers and through integrations with Syslog or the XML API, which have the added benefit of allowing you to safely capture user mapping information from any device type or operating system, instead of just Windows clients.

The complete procedure to configure the PAN-OS integrated User-ID agent to probe clients requires additional tasks besides configuring the client probing settings.

The PAN-OS Integrated User-ID agent does not support NetBIOS probing but the Windows-based User-ID agent does support it.

Client Probing Settings	Description
Enable Probing	Select this option to enable WMI probing.
Probe Interval (min)	Enter the probe interval in minutes (range is 1-1440; default is 20). This is the interval between when the firewall finishes processing the last request and when it starts the next request. In large deployments, it is important to set the interval properly to allow time to probe each client that the user mapping process identified. Example, if you have 6,000 users and an interval of 10 minutes, it would require 10 WMI requests per second from each client. *If the probe request load is high, the observed delay between requests might significantly exceed the interval you specify.*

Cache

- **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Cache**

To ensure that the firewall has the most current user mapping information as users roam and obtain new IP addresses, configure timeouts for clearing user mappings from the firewall cache. This timeout applies to user mappings learned through any method except Authentication Portal. For mappings learned through Authentication Portal, set the timeout in the Authentication Portal Settings (Device > User Identification > Authentication Portal Settings, **Timer** and **Idle Timer** fields).

To match usernames collected from User-ID sources even if a domain is not included, configure the firewall to allow matching usernames without domains. You should only use this option if the usernames in your organization are not duplicated across domains.

Cache Settings	Description
Enable User Identification Timeout	Select this option to enable a timeout value for user mapping entries. When the timeout value is reached for an entry, the firewall clears it and collects a new mapping. This ensures that the firewall has the most current information as users roam and obtain new IP addresses. *Enable the timeout to ensure the firewall has the most current user-to-IP-address mapping information.*
User Identification Timeout (min)	Set the timeout value in minutes for user mapping entries (range is 1 to 3,600; default is 45). *Set the timeout value to the half-life of the DHCP lease or to the Kerberos ticket lifetime.* *If you configure firewalls to redistribute mapping information, each firewall clears the mapping entries it*

Cache Settings	Description
	receives based on the timeout you set on that firewall, not on the timeouts set in the forwarding firewalls.
Allow matching usernames without domains	Select this option to allow the firewall to match users if the domain is not provided by the User-ID source. To prevent users from being misidentified, only select this option if your usernames are not duplicated across domains. *Before you enable this option, verify that the firewall has fetched the group mappings from the LDAP server.*

Redistribution

- **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Redistribution**

To enable a firewall or virtual system to serve as a User-ID agent that redistributes user mapping information along with the timestamps associated with authentication challenges, configure the settings described in the following table. When you later connect this firewall to an appliance (such as Panorama) that will receive the mapping information and timestamps, the appliance uses these fields to identify the firewall or virtual system as a User-ID agent.

The complete procedure to configure firewalls to redistribute user mapping information and authentication timestamps requires additional tasks besides specifying the redistribution settings.

By default, a firewall with multiple virtual systems doesn't redistribute user mapping information across its virtual systems, though you can configure them for redistribution.

Redistribution Settings	Description
Collector Name	Enter a collector name (up to 255 alphanumeric characters) to identify the firewall or virtual system as a User-ID agent.
Pre-Shared Key/Confirm Pre-Shared Key	Enter a pre-shared key (up to 255 alphanumeric characters) to identify the firewall or virtual system as a User-ID agent.

Syslog Filters

- **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Syslog Filters**

The User-ID agent uses Syslog Parse profiles to filter syslog messages sent from the syslog senders that the agent monitors for IP address-to-username mapping information (see Configure Access to Monitored Servers). Each profile can parse syslog messages for either of the following event types, but not both:

- Authentication (login) events—Used to add user mappings to the firewall.
- Logout events—Used to delete user mappings that are no longer current. Deleting outdated mappings is useful in environments where IP address assignments change often.

Palo Alto Networks provides the firewall with predefined Syslog Parse profiles through Applications content updates. To dynamically update the list of profiles as vendors develop new filters, schedule these dynamic content updates (see Device > Dynamic Updates). The predefined profiles are global to the firewall, whereas the custom profiles you configure apply only to the virtual system (**Location**) selected under **Device** > **User Identification** > **User Mapping**.

Syslog messages must meet the following criteria for a User-ID agent to parse them:

- Each message must be a single-line text string. A new line (\n) or a carriage return plus a new line (\r\n) are the delimiters for line breaks.
- The maximum size for individual messages is 8,000 bytes.
- Messages sent over UDP must be contained in a single packet; messages sent over SSL can span multiple packets. A single packet might contain multiple messages.

To configure a custom profile, click **Add** and specify the settings described in the following table. The field descriptions in this table use a login event example from a syslog message with the following format:

```
[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success User:domain
\johndoe_4 Source:192.168.0.212
```

The complete procedure to configure the User-ID agent to parse a syslog sender for user mapping information requires additional tasks besides creating a Syslog Parse profile.

Field	Description
Syslog Parse Profile	Enter a name for the profile (up to 63 alphanumeric characters).
Description	Enter a description for the profile (up to 255 alphanumeric characters).
Type	Specify the type of parsing for filtering the user mapping information: • **Regex Identifier**—Use **Event Regex**, **Username Regex**, and **Address Regex** to specify regular expressions (regex) that describe search patterns for identifying and extracting user mapping information from syslog messages. The firewall uses the regex to match authentication or logout events in syslog messages and to match the usernames and IP addresses within matching messages. • **Field Identifier**—Use the **Event String**, **Username Prefix**, **Username Delimiter**, **Address Prefix**, **Address Delimiter**, and **Addresses Per Log** fields to specify strings for matching the authentication or logout event and for identifying the user mapping information in syslog messages. The remaining fields in the dialog vary based on your selection. Configure the fields as described in the following rows.
Event Regex	Enter the regex for identifying successful authentication or logout events. For the example message used with this table, the regex **`(authentication\ success) {1}`** extracts the first **`{1}`** instance of the string `authentication success`. The backslash before the space is a standard regex escape character that instructs the regex engine not to treat the space as a special character.
Username Regex	Enter the regex for identifying the username field in authentication success or logout messages. For the example message used with

Field	Description
	this table, the regex **`User:([a-zA-Z0-9\\\._]+)`** would match the string `User:johndoe_4` and extract acme\johndoe1 as the username.
Address Regex	Enter the regex to identify the IP address portion of authentication success or logout messages. In the example message used with this table, the regular expression **`Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})`** matches the IPv4 address `Source:192.168.0.212` and adds 192.168.0.212 as the IP address in the username mapping.
Event String	Enter a matching string to identify authentication success or logout messages. For the example message used with this table, you would enter the string **`authentication success`**.
Username Prefix	Enter the matching string to identify the beginning of the username field within authentication or logout syslog messages. The field does not support regex expressions such as **`\s`** (for a space) or **`\t`** (for a tab). In the example message used with this table, `User:` identifies the start of the username field.
Username Delimiter	Enter the delimiter that marks the end of the username field within an authentication or logout message. Use \s to indicate a standalone space (as in the example message) and \t to indicate a tab.
Address Prefix	Enter a matching string to identify the start of the IP address field in syslog messages. The field does not support regex expressions such as **`\s`** (for a space) or **`\t`** (for a tab). In the example message used with this table, `Source:` identifies the start of the address field.
Address Delimiter	Enter the matching string that marks the end of the IP address field within authentication success or logout messages. For example, enter **`\n`** to indicate the delimiter is a line break.
Addresses Per Log	Enter the maximum number of IP addresses that you want the firewall to parse (default is 1; range is 1—3).

Ignore User List

- **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Ignore User List**

The ignore user list defines which user accounts don't require IP address-to-username mapping (for example, kiosk accounts). To configure the list, click **Add** and enter a username. You can use an asterisk as a wildcard character to match multiple usernames but only as the last character in the entry. For example, **corpdomain\it-admin*** matches all administrators in the **corpdomain** domain whose usernames start with the string **it#admin**. You can add up to 5,000 entries to exclude from user mapping.

Define the ignore user list on the firewall that is the User-ID agent, not the client. If you define the ignore user list on the client firewall, the users in the list are still mapped during redistribution.

Monitor Servers

- Device > User Identification > User Mapping

Use the Server Monitoring section to define the Microsoft Exchange Servers, Active Directory (AD) domain controllers, Novell eDirectory servers, or syslog senders that the User-ID agent monitors for login events.

- Configure Access to Monitored Servers
- Manage Access to Monitored Servers
- Include or Exclude Subnetworks for User Mapping

Configure Access to Monitored Servers

Use the Server Monitoring section to **Add** server profiles that specify the servers the firewall will monitor.

Configure at least two User-ID monitored servers so if a server goes down, the firewall can still learn IP-address-to-username mappings.

The complete procedure to configure the PAN-OS integrated User-ID agent to monitor servers requires additional tasks besides creating server profiles.

Server Monitoring Settings	Description
Name	Enter a name for the server.
Description	Enter a description of the server.
Enabled	Select this option to enable log monitoring for this server.
Type	Select the server type. Your selection determines which other fields this dialog displays. • **Microsoft Active Directory** • **Microsoft Exchange** • **Novell eDirectory** • **Syslog Sender**
Transport Protocol (Microsoft Active Directory and Microsoft Exchange only)	Select the transport protocol: • **WMI**—(default) Use Windows Management Instrumentation (WMI) to probe each learned IP address and verify that the same user is still logged in. • **Win-RM-HTTP**—Use Windows Remote Management (WinRM) over HTTP to monitor the security logs and session information on the server. This option requires the Kerberos **Domain's DNS Name** in the Server Monitor Account. • **Win-RM-HTTPS**—Use Windows Remote Management (WinRM) over HTTPS to monitor the security logs and session information on the server. To require server certificate validation with the Windows server when using Kerberos authentication, make sure you configure NTP in the Global Services Settings and select the Root CA as the certificate profile (Device > User Identification > Connection Security).

Server Monitoring Settings	Description
Network Address	Enter the server IP address or FQDN for the monitored server. If you use Kerberos for server authentication, you must enter an FQDN. This option is not supported when the **Type** is **Novell eDirectory**.
Server Profile (Novell eDirectory only)	Select an LDAP server profile for connecting to the Novell eDirectory server (Device > Server Profiles > LDAP).
Connection Type (Syslog Sender only)	Select whether the User-ID agent listens for syslog messages on the **UDP** port (514) or the **SSL** port (6514). If you select **SSL**, the **Syslog Service Profile** you select when you enable Server Monitoring determines which SSL/TLS versions are allowed and the certificate that the firewall uses to secure a connection to the syslog sender.  *As a security best practice, select SSL when using the PAN-OS integrated User-ID agent to map IP addresses to usernames. If you select UDP, ensure that the syslog sender and client are both on a dedicated, secure network to prevent untrusted hosts from sending UDP traffic to the firewall.*
Filter (Syslog Sender only)	If the server **Type** is **Syslog Sender**, then **Add** one or more Syslog Parse profiles to use for extracting usernames and IP addresses from the syslog messages received from this server. You can add a custom profile (see Syslog Filters) or a predefined profile. For each profile, set the **Event Type**: • **login**—The User-ID agent parses syslog messages for login events to create user mappings. • **logout**—The User-ID agent parses syslog messages for logout events to delete user mappings that are no longer current. In networks where IP address assignment is dynamic, automatic deletion improves the accuracy of user mappings by ensuring that the agent maps each IP address only to the currently associated user.  *If you add a predefined Syslog Parse profile, check its name to determine whether it is intended to match login or logout events.*
Default Domain Name (Syslog Sender only)	(Optional) If the server **Type** is **Syslog Sender**, enter a domain name to override the current domain name in the username of your syslog message or prepend the domain to the username if your syslog message doesn't contain a domain.

Manage Access to Monitored Servers

Perform the following tasks in the Server Monitoring section to manage access to the servers that the User-ID agent monitors for user mapping information.

Task	Description
Display server information	For each monitored server, the User Mapping page displays the Status of the connection from the User-ID agent to the server. After you **Add** a server, the firewall tries to connect to it. If the connection attempt is successful, the Server Monitoring section displays Connected in the Status column. If the firewall cannot connect, the Status column displays an error condition, such as `Connection refused` or `Connection timeout`. For details on the other fields that the Server Monitoring section displays, see Configure Access to Monitored Servers.
Add	To Configure Access to Monitored Servers, **Add** each server that the User-ID agent will monitor for user mapping information.
Delete	To remove a server from the user mapping process (discovery), select the server and **Delete** it. **Tip**: To remove a server from discovery without deleting its configuration, edit the server entry and clear **Enabled**.
Discover	You can automatically **Discover** Microsoft Active Directory domain controllers using DNS. The firewall will discover domain controllers based on the domain name entered in the **Device** > **Setup** > **Management** page, **General Settings** section, **Domain** field. After discovering a domain controller, the firewall creates an entry for it in the Server Monitoring list; you can then enable the server for monitoring. *The Discover feature works for domain controllers only, not Exchange servers or eDirectory servers.*

Include or Exclude Subnetworks for User Mapping

- Device > User Identification > User Mapping

Use the Include/Exclude Networks list to define the subnetworks that the User-ID agent will include or exclude when performing IP address-to-username mapping (discovery). By default, if you don't add any subnetworks to the list, the User-ID agent performs discovery for user identification sources in all subnetworks except when using WMI probing for client systems that have public IPv4 addresses. (Public IPv4 addresses are those outside the scope of RFC 1918 and RFC 3927).

To enable WMI probing for public IPv4 addresses, you must add their subnetworks to the list and set their **Discovery** option to **Include**. If you configure the firewall to redistribute user mappinginformation to other firewalls, the discovery limits you specify in the list will apply to the redistributed information.

Use the include and exclude lists to define the subnets in which the firewall performs user mapping.

You can perform the following tasks on the Include/Exclude Networks list:

Task	Description
Add	To limit discovery to a specific subnetwork, **Add** a subnetwork profile and complete the following fields:

Task	Description
	• **Name**—Enter a name to identify the subnetwork. • **Enabled**—Select this option to enable inclusion or exclusion of the subnetwork for server monitoring. • **Discovery**—Select whether the User-ID agent will **Include** or **Exclude** the subnetwork. • **Network Address**—Enter the IP address range of the subnetwork. The User-ID agent applies an implicit exclude all rule to the list. For example, if you add subnetwork 10.0.0.0/8 with the **Include** option, the User-ID agent excludes all other subnetworks even if you don't add them to the list. Add entries with the **Exclude** option only if you want the User-ID agent to exclude a subset of the subnetworks you explicitly included. For example, if you add 10.0.0.0/8 with the **Include** option and add 10.2.50.0/22 with the **Exclude** option, the User-ID agent will perform discovery on all the subnetworks of 10.0.0.0/8 except 10.2.50.0/22, and will exclude all subnetworks outside of 10.0.0.0/8. If you add **Exclude** profiles without adding any **Include** profiles, the User-ID agent excludes all subnetworks, not just the ones you added.
Delete	To remove a subnetwork from the list, select and **Delete** it. **Tip**: To remove a subnetwork from the Include/Exclude Networks list without deleting its configuration, edit the subnetwork profile and clear **Enabled**.
Custom Include/ Exclude Network	By default, the User-ID agent evaluates the subnetworks in the order you add them, from top-first to bottom-last. To change the evaluation order, click **Custom Include/ Exclude Network Sequence**. You can then **Add**, **Delete**, **Move Up**, or **Move Down** the subnetworks to create a custom evaluation order.

Device > User Identification > Connection Security

Edit ( ) the User-ID Connection Security settings to select the certificate profile used by the firewall to validate the certificate presented by Windows User-ID agents. The firewall uses the selected certificate profile to verify the identity of the User-ID agent by validating the server certificate presented by the agent.

Task	Description
User-ID Certificate Profile	From the drop-down, select the certificate profile to use when authenticating Windows User-ID agents or select New Certificate Profile to create a new certificate profile. Select **None** to remove the certificate profile and use default authentication instead. To require server certificate validation with the Windows server when you Configure Access to Monitored Servers using Kerberos for server authentication, make sure you configure NTP in the Global Services Settings and select the Root CA as the certificate profile.
Remove All (Template Configuration Only)	Removes the certificate profile attached to the User-ID Connection Security configuration for the selected template.

Device > User Identification > Terminal Server Agents

On a system that supports multiple users who share the same IP address, a Terminal Server (TS) agent identifies individual users by allocating port ranges to each one. The TS agent informs every connected firewall of the allocated port range so that the firewalls can enforce policy based on users and user groups.

All firewall models can collect username-to-port mapping information from up to 5,000 multi-user systems. The number of TS agents from which a firewall can collect the mapping information varies by firewall model.

You must install and configure the TS agents before configuring access to them. The complete procedure to configure user mapping for terminal server users requires additional tasks besides configuring connections to TS agents.

You can perform the following tasks to manage access to TS agents.

Task	Description
Display information / Refresh Connected	In the **Terminal Server Agents** page, the Connected column displays the status of the connections from the firewall to the TS agents. A green icon indicates a successful connection, a yellow icon indicates a disabled connection, and a red icon indicates a failed connection. If you think the connection status might have changed since you first opened the page, click **Refresh Connected** to update the status display.
Add	To configure access to a TS agent, **Add** an agent and configure the following fields: • **Name**—Enter a name to identify the TS agent (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. • **Host**—Enter the static IP address or hostname of the terminal server where the TS agent is installed. • **Port**—Enter the port number (default is 5009) that the TS agent service uses to communicate with the firewall. • **Alternative Hosts**—If the terminal server where the TS agent is installed has multiple IP addresses that can appear as the source IP address for the outgoing traffic, **Add** and enter up to eight additional static IP addresses or hostnames. • **Enabled**—Select this option to enable the firewall to communicate with this TS agent.
Delete	To remove the configuration that enables access to a TS agent, select the agent and click **Delete**. *To disable access to a TS agent without deleting its configuration, edit the agent and clear the Enabled option.*
PDF/CSV	Administrative roles with a minimum of read-only access can export the device configuration table as **PDF/CSV**. You can apply filters to create more specific table

Task	Description
	configuration outputs for things such as audits. Only visible columns in the web interface will be exported. See Configuration Table Export.

Device > User Identification > Group Mapping Settings Tab

- **Device** > **User Identification** > **Group Mapping Settings**

To base security policies and reports on users and user groups, the firewall retrieves the list of groups and the corresponding list of members specified and maintained on your directory servers. The firewall supports a variety of LDAP directory servers, including the Microsoft Active Directory (AD), the Novell eDirectory, and the Sun ONE Directory Server.

The number of distinct user groups that each firewall or Panorama can reference across all policies varies by model. Regardless of model, though, you must configure an LDAP server profile (Device > Server Profiles > LDAP) before you can create a group mapping configuration.

The complete procedure for mapping usernames to groups requires additional tasks besides creating group mapping configurations.

Add and configure the following fields as needed to create a group mapping configuration. To remove a group mapping configuration, select and **Delete** it. If you want to disable a group mapping configuration without deleting it, edit the configuration and clear the **Enabled** option.

If you create multiple group mapping configurations that use the same base distinguished name (DN) or LDAP server, the group mapping configurations cannot contain overlapping groups (for example, the Include list for one group mapping configuration cannot contain a group that is also in a different group mapping configuration).

Group Mapping Settings—Server Profile	Configured In	Description
Name	**Device** > **User Identification** > **Group Mapping Settings**	Enter a name to identify the group mapping configuration (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Server Profile	**Device** > **User Identification** > **Group Mapping Settings** > **Server Profile**	Select the LDAP server profile to use for group mapping on this firewall.
Update Interval		Specify the interval in seconds after which the firewall will initiate a connection with the LDAP directory server to obtain any updates that were made to the groups that firewall policies use (range is 60 to 86,400).
User Domain		By default, **User Domain** is blank: the firewall automatically detects the domain names for Active Directory servers. If you enter a value, it overrides any domain names that the firewall retrieves from the LDAP source. Your entry must be the NetBIOS name.

Group Mapping Settings—Server Profile	Configured In	Description
		This field affects only the usernames and group names retrieved from the LDAP source. To override the domain associated with a username for user authentication, configure the User Domain and Username Modifier for the authentication profile you assign to that user (see Device > Authentication Profile).
Group Objects		• **Search Filter**—Enter an LDAP query that specifies which groups to retrieve and track. • **Object Class**—Enter a group definition. The default is objectClass=group, which specifies that the system retrieves all objects in the directory that match the group **Search Filter** and have objectClass=group.
User Objects		• **Search Filter**—Enter an LDAP query that specifies which users to retrieve and track. • **Object Class**—Enter a user object definition. For example, in Active Directory, the objectClass is *user*.
Enabled		Select this option to enable server profile for group mapping.
Fetch list of managed devices		For GlobalProtect deployments, select this option to allow the firewall to retrieve serial numbers from a directory server (such as Active Directory). This enables GlobalProtect to identify the status of connecting endpoints and enforce HIP-based security policies based on the presence of the endpoint serial number.
User Attributes	**Device > User Identification > Group Mapping Settings > User and Group Attributes**	Specify the directory attributes to identify users: • **Primary Username**—Specify the attribute the User-ID source provides for the username (for example, **`userPrincipalName`** or **`sAMAccountName`**) *The primary username is how the firewall identifies the user in logs, reports, and policy configurations, even if the firewall receives other formats from the User-ID*

Group Mapping Settings—Server Profile	Configured In	Description
		sources. If you do not specify a format, the firewall uses the `sAMAccountName` format by default for Active Directory and the `uid` format for Novell eDirectory and Sun ONE Directory Server. • **E-Mail**—Specify the attribute the User-ID source provides for the email address. The default is **`mail`**. • **Alternate Username 1-3**—Specify up to three additional attributes that correspond with the formats your User-ID sources can send.  *If you configure an Active Directory server, the Alternate Username 1 is `userPrincipalName` by default.*
Group Attributes		Specify the attributes that the User-ID sources use to identify groups: • **Group Name**—Specify the attribute the User-ID source uses for the group name attribute. The default for Active Directory is `name` and the default for Novell eDirectory or Sun ONE Directory Server is `cn`. • **Group Member**—Specify the attribute the User-ID source uses for the group member. The default is `member`. • **E-Mail**—Specify the attribute the User-ID source uses for the email address. The default is `mail`.
Available Groups Included Groups	**Device** > **User Identification** > **Group Mapping Settings** > **Group Include List**	Use these fields to limit the number of groups that the firewall displays when you create a security rule. Browse the LDAP tree to find the groups you want to use in rules. To include a group, select and add (⊕) it in the Available Groups list. To remove a group from the list, select and delete (⊖) it from the Included Groups list.  *Include only the groups you need so that the firewall retrieves user group mappings for only the necessary groups*

Group Mapping Settings—Server Profile	Configured In	Description
		and not for the whole tree from the LDAP directory.
Name LDAP Filter	**Device** > **User Identification** > **Group Mapping Settings** > **Custom Group**	Create custom groups based on LDAP filters so that you can base firewall policies on user attributes that don't match existing user groups in the LDAP directory. The User-ID service maps all the LDAP directory users who match the filter to the custom group. If you create a custom group with the same Distinguished Name (DN) as an existing Active Directory group domain name, the firewall uses the custom group in all references to that name (for example, in policies and logs). To create a custom group, **Add** and configure the following fields: • **Name**—Enter a custom group name that is unique in the group mapping configuration for the current firewall or virtual system. • **LDAP Filter**—Enter a filter of up to 2,048 characters.  *Use only indexed attributes in the filter to expedite LDAP searches and minimize the performance impact on the LDAP directory server; the firewall does not validate LDAP filters.* The combined maximum for the **Included Groups** and **Custom Group** lists is 640 entries. To delete a custom group, select and **Delete** it. To make a copy of a custom group, select and **Clone** it and then edit the fields as appropriate.  *After adding or cloning a custom group, you must Commit your changes before your new custom group is available in policies and objects.*

Device > User Identification > Authentication Portal

Edit ( ) the Authentication Portal Settings to configure the firewall to authenticate users whose traffic matches an Authentication policy rule.

If Authentication Portal uses an SSL/TLS Service profile (Device > Certificate Management > SSL/TLS Service Profile), authentication profile (Device > Authentication Profile), or Certificate Profile (Device > Certificate Management > Certificate Profile), then configure the profile before you begin. The complete procedure to configure Authentication Portal requires additional tasks in addition to configuring these profiles.

You must Enable Authentication Portal to enforce Authentication policy (see Policies > Authentication).

Field	Description
Enable Authentication Portal	Select this option to enable Authentication Portal.
Idle Timer (min)	Enter the user time-to-live (TTL) value in minutes for a Authentication Portal session (range is 1 to 1,440; default is 15). This timer resets every time there is activity from an Authentication Portal user. If idle time for a user exceeds the **Idle Timer** value, PAN-OS removes the Authentication Portal user mapping and the user must log in again.
Timer (min)	This is the maximum TTL in minutes, which is the maximum time that any Authentication Portal session can remain mapped (range is 1 to 1,440; default is 60). After this duration elapses, PAN-OS removes the mapping and users must re-authenticate even if the session is active. This timer prevents stale mappings and overrides the **Idle Timer** value. *You should always set the expiration Timer higher than the Idle Timer.*
SSL/TLS Service Profile	To specify a firewall server certificate and the allowed protocols for securing redirect requests, select an SSL/TLS service profile (Device > Certificate Management > SSL/TLS Service Profile). If you select **None**, the firewall uses its local default certificate for SSL/TLS connections. *In the SSL/TLS Service Profile, set the Min Version to TLSv1.2 and set the Max Version to Max to provide the strongest security against SSL/TLS protocol vulnerabilities. Setting the Max Version to Max ensures that as stronger protocols become available, the firewall always uses the latest version.*

Field	Description
	To transparently redirect users without displaying certificate errors, assign a profile associated with a certificate that matches the IP address of the interface to which you are redirecting web requests.
Authentication Profile	You can select an authentication profile (Device > Authentication Profile) to authenticate users when their traffic matches an Authentication policy rule (Policies > Authentication). However, the authentication profile you select in the Authentication Portal Settings applies only to rules that reference one of the default authentication enforcement objects (Objects > Authentication). This is typically the case right after an upgrade to PAN-OS 8.0 because all Authentication rules initially reference the default objects. For rules that reference custom authentication enforcement objects, select the authentication profile when you create the object.
GlobalProtect Network Port for Inbound Authentication Prompts (UDP)	Specify the port that GlobalProtect™ uses to receive inbound authentication prompts from multi-factor (MFA) gateways. (range is 1 to 65,536; default is 4,501). To support multi-factor authentication, a GlobalProtect endpoint must receive and acknowledge UDP prompts that are inbound from the MFA gateway. When a GlobalProtect endpoint receives a UDP message on the specified network port and the UDP message comes from a trusted firewall or gateway, GlobalProtect displays the authentication message (seeCustomize the GlobalProtect App).
Mode	Select how the firewall captures web requests for authentication: • **Transparent**—The firewall intercepts web requests according to the Authentication rule and impersonates the original destination URL, issuing an HTTP 401 message to prompt the user to authenticate. However, because the firewall does not have the real certificate for the destination URL, the browser displays a certificate error to users attempting to access a secure site. Therefore, only use this mode when absolutely necessary, such as in Layer 2 or virtual wire deployments. • **Redirect**—The firewall intercepts web requests according to the Authentication rule and redirects them to the specified Redirect Host. The firewall uses an HTTP 302 redirect to prompt the user to authenticate. The best practice is to use **Redirect** because it provides a better end-user experience (displays no certificate errors and allows session cookies that make browsing seamless because **Redirect** doesn't remap when timeouts expire). However, it requires that you enable response pages on the Interface Management profile assigned to the ingress Layer 3 interface (for details, see Network > Network Profiles > Interface Mgmt and PA-7000 Series Layer 3 Interface). Another benefit of the Redirect mode is that it allows for session cookies, which enable the user to continue browsing to authenticated sites without requiring re-mapping each time the timeouts expire. This is especially useful for users who roam from one IP address to another (for example, from the corporate LAN to the wireless network) because they don't need to re-authenticate when their IP address changes as long as the session stays open. *Redirect mode is required if Authentication Portal uses Kerberos SSO because the browser provides credentials only to trusted sites. Redirect mode is also required if Authentication Portal uses multi-factor authentication (MFA).*
Session Cookie	• **Enable**—Select this option to enable session cookies.

Field	Description
(Redirect mode only)	• **Timeout**—If you **Enable** session cookies, this timer specifies the number of minutes for which the cookie is valid (range is 60–10,080; default is 1,440). *Set the timeout value short enough so that it doesn't lead to stale user mapping entries in cookies but long enough to promote a good user experience by not prompting users to log in multiple times during a session. Start with a value less than or equal to 480 minutes (8 hours) and adjust the value as necessary.* • **Roaming**—Select this option to retain the cookie if the IP address changes while the session is active (such as when the endpoint moves from a wired to a wireless network). The user must re-authenticate only if the cookie times out or the user closes the browser.
Redirect Host (Redirect mode only)	Specify the intranet hostname that resolves to the IP address of the Layer 3 interface to which the firewall redirects web requests. *If users authenticate through Kerberos single sign-on (SSO), the Redirect Host must be the same as the hostname specified in the Kerberos keytab.*
Certificate Profile	You can select a Certificate Profile (Device > Certificate Management > Certificate Profile) to authenticate users when their traffic matches any Authentication policy rule (Policies > Authentication). For this authentication type, Authentication Portal prompts the endpoint browser of the user to present a client certificate. Therefore, you must deploy client certificates to each user system. Furthermore, on the firewall, you must install the certificate authority (CA) certificate that issued the client certificates and assign the CA certificate to the Certificate Profile. This is the only authentication method that enables **Transparent** authentication for macOS and Linux endpoints.

GlobalProtect

GlobalProtect™ provides a complete infrastructure for managing your mobile workforce to enable secure access for all of your users, regardless of what devices they are using or where they are located. The following firewall web interface pages allow you to configure and manage GlobalProtect components:

- Network > GlobalProtect > Portals
- Network > GlobalProtect > Gateways
- Network > GlobalProtect > MDM
- Network > GlobalProtect > Device Block List
- Network > GlobalProtect > Clientless Apps
- Network > GlobalProtect > Clientless App Groups
- Objects > GlobalProtect > HIP Objects
- Objects > GlobalProtect > HIP Profiles
- Device > GlobalProtect Client

Looking for more?

See the GlobalProtect Administrator's Guide to learn more about GlobalProtect, including details on setting up the GlobalProtect infrastructure, how to use host information to enforce policy, and step-by-step instructions for configuring common GlobalProtect deployments.

Network > GlobalProtect > Portals

Select **Network** > **GlobalProtect** > **Portals** to set up and manage a GlobalProtect™ portal. The portal provides the management functions for the GlobalProtect infrastructure. Every endpoint that participates in the GlobalProtect network receives its configuration from the portal, including information about the available gateways and any client certificates that are necessary for the app to connect to a gateway. In addition, the portal controls the behavior and distribution of the GlobalProtect app software to macOS and Windows endpoints. For Linux endpoints, you must obtain the software from the Support Site; for mobile devices, the GlobalProtect app is distributed through the Apple App Store (for iOS devices), through Google Play (for Android devices), and through the Microsoft Store (for Windows Phone and other Windows UWP devices), and, for Chromebooks, the GlobalProtect app is distributed by the Chromebook Management Console or through Google Play.

To add a portal configuration, click **Add** to open the GlobalProtect Portal dialog.

What are you looking for?	See:
What general settings should I configure for the GlobalProtect portal?	GlobalProtect Portals General Tab
How can I assign an authentication profile to a portal configuration?	GlobalProtect Portals Authentication Tab
How can I define the data that the GlobalProtect app collects from endpoints?	GlobalProtect Portals Portal Data Collection Tab
What client authentication options can I configure?	GlobalProtect Portals Agent Authentication Tab
How can I assign a configuration to a specific group of devices based on operating system, user, and/or user group?	GlobalProtect Portals Agent Config Selection Criteria Tab
How can I configure the settings and priority of the internal gateways?	GlobalProtect Portals Agent Internal Tab
How can I configure the settings and priority of the external gateways?	GlobalProtect Portals Agent External Tab
How can I create separate client configurations for different types of users?	GlobalProtect Portals Agent Tab
What settings can I customize on the look and behavior of the GlobalProtect app?	GlobalProtect Portals Agent App Tab
How can I configure data collection options?	GlobalProtect Portals Agent Data Collection Tab

What are you looking for?	See:
How can I configure the GlobalProtect portal to allow access to web applications without installing the GlobalProtect app?	GlobalProtect Portals Clientless VPN Tab
How can I extend VPN connectivity to a firewall which acts as a satellite?	GlobalProtect Portal Satellite Tab
Looking for more?	For detailed, step-by-step instructions on setting up the portal, refer to Configure a GlobalProtect Portal in the *GlobalProtect Administrator's Guide*.

GlobalProtect Portals General Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **General**

Select the **General** tab to define the network settings that the GlobalProtect app uses to connect to the GlobalProtect portal. Optionally, you can disable the login page or specify a custom portal login and help pages for GlobalProtect. For information on how to create and import custom pages, refer to Customize the Portal Login, Welcome, and HelpPages in the GlobalProtect Administrator's Guide.

GlobalProtect Portal Settings	Description
Name	Type a name for the portal (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in multiple virtual system mode, the **Location** is the virtual system (vsys) where the GlobalProtect portal is available. For a firewall that is not in multi-vsys mode, **Location** selection is not available. After you save the portal, you cannot change **Location**.
Network Settings	
Interface	Select the name of the firewall interface that will be the ingress for communications from remote endpoints and firewalls. *Do not attach an interface management profile that allows Telnet, SSH, HTTP, or HTTPS to an interface where you have configured a GlobalProtect portal or gateway because this will expose the management interface to the internet. Refer to Best Practices for Securing Administrative Access for more details on how to protect access to your management network.*
IP Address	Specify the IP address on which to run the GlobalProtect portal web service. Select the **IP Address Type** and then enter the **IP Address**. • The IP address type can be **IPv4** (for IPv4 traffic only), **IPv6** (for IPv6 traffic only), or **IPv4 and IPv6**. Use **IPv4 and IPv6** if your network

GlobalProtect Portal Settings	Description
	supports dual stack configurations, where IPv4 and IPv6 run at the same time. • The IP address must be compatible with the IP address type. For example, 172.16.1.0 for IPv4 or 21DA:D3:0:2F3b for IPv6. • If you choose **IPv4 and IPv6**, enter the appropriate IP address type for each.
Log Settings	
Log Successful SSL Handshake	(Optional) Creates detailed logs of successful SSL Decryption handshakes. Disabled by default.  *Logs consume storage space. Before you log successful SSL handshakes, ensure you have the resources available to store the logs. Edit Device > Setup > Management > Logging and Reporting Settings to check the current log memory allocation to and re-allocate log memory among log types.*
Log Unsuccessful SSL Handshake	Creates detailed logs of unsuccessful SSL Decryption handshakes so you can find the cause of decryption issues. Enabled by default.  *Logs consume storage space. To allocate more (or less) log storage space to Decryption logs, edit the log memory allocation (Device > Setup > Management > Logging and Reporting Settings).*
Log Forwarding	Specify the method and location to forward GlobalProtect SSL handshake (decryption) logs.
Appearance	
Portal Login Page	(Optional) Choose a custom login page for user access to the portal. You can select the **factory-default** page or **Import** a custom page. The default is **None**. To prevent access to this page from a web browser, **Disable** this page.
Portal Landing Page	(Optional) Choose a custom landing page for the portal. You can select the **factory-default** page or **Import** a custom page. The default is **None**.
App Help Page	(Optional) Choose a custom help page to assist the user with GlobalProtect. You can select the **factory-default** page or **Import** a custom page. The factory-default help page is provided with the GlobalProtect app software. If you select a custom help page, the GlobalProtect portal provides the help page with the GlobalProtect portal configuration. When you leave the default value of **None**, the GlobalProtect app suppresses the page and removes the option from the menu.

GlobalProtect Portals Authentication Configuration Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Authentication**

Select the **Authentication** tab to configure the various GlobalProtect™ portal settings:

- An SSL/TLS service profile that the portal and servers use for authentication. The service profile is independent of the other settings in Authentication.
- Unique authentication schemes that are based primarily on the operating system of the user endpoints and secondarily on an optional authentication profile.
- (Optional) A **Certificate Profile**, which enables GlobalProtect to use a specific certificate profile for authenticating the user. The certificate from the client must match the certificate profile (if client certificates are part of the security scheme).

GlobalProtect Portal Authentication Settings	Description
Server Authentication	
SSL/TLS Service Profile	Select an existing SSL/TLS Service profile. The profile specifies a certificate and the allowed protocols for securing traffic on the management interface. The Common Name (CN) and, if applicable, the Subject Alternative Name (SAN) fields of the certificate associated with the profile must match the IP address or FQDN of the **Interface** selected in the **General** tab.  *In GlobalProtect VPN configurations, use a profile associated with a certificate from a trusted third-party CA or a certificate that your internal enterprise CA generated.*
Client Authentication	
Name	Enter a name to identify the client authentication configuration. (The client authentication configuration is independent of the SSL/TLS service profile.) You can create multiple client authentication configurations and differentiate them primarily by operating system and additionally by unique authentication profiles (for the same OS). For example, you can add client authentication configurations for different operating systems but also have different configurations for the same OS that are differentiated by unique authentication profiles. (You should manually order these profiles from most specific to most general. For example, all users and any OS is the most general.) You can also create configurations that GlobalProtect deploys to apps in **Pre-logon** mode (before the user has logged in to the system) or that it applies to any user. (Pre-logon establishes a VPN tunnel to a GlobalProtect gateway before the user logs in to GlobalProtect.)
OS	To deploy a client authentication profile specific to the operating system (OS) on an endpoint, **Add** the OS (**Any**, **Android**, **Chrome**, **iOS**, **Linux**, **Mac**, **Windows**, or **WindowsUWP**). The OS is the primary differentiator between configurations. (See Authentication Profile for further differentiation.) The additional options of **Browser** and **Satellite** enable you to specify the authentication profile to use for specific scenarios. Select **Browser** to specify the authentication profile to use to authenticate a user accessing the portal

GlobalProtect Portal Authentication Settings	Description
	from a web browser with the intent of downloading the GlobalProtect app (Windows and Mac). Select **Satellite** to specify the authentication profile to use to authenticate the satellite (LSVPN).
Authentication Profile	In addition to distinguishing a client authentication configuration by an OS, you can further differentiate by specifying an authentication profile. (You can create a **New Authentication Profile** or select an existing one.) To configure multiple authentication options for an OS, you can create multiple client authentication profiles.  *If you are configuring an LSVPN in Gateways, you cannot save that configuration unless you select an authentication profile here. Also, if you plan to use serial numbers to authenticate satellites, the portal must have an authentication profile available when it cannot locate or validate a firewall serial number.* See also Device > Authentication Profile.
Username Label	Specify a custom username label for GlobalProtect portal login. For example, **Username (only)** or **Email Address (username@domain)**.
Password Label	Specify a custom password label for GlobalProtect portal login. For example, **Password (Turkish)** or **Passcode** (for two-factor, token-based authentication).
Authentication Message	To help end users know the type of credentials they need for logging in, enter a message or keep the default message. The maximum length of the message is 256 characters.
Allow Authentication with User Credentials OR Client Certificate	If you select **No**, users must authenticate to the gateway using both user credentials and client certificates. If you select **Yes**, users can authenticate to the gateway using either user credentials or client certificates.
Certificate Profile	
Certificate Profile	(Optional) Select the **Certificate Profile** the portal uses to match those client certificates that come from user endpoints. With a Certificate Profile, the portal authenticates the user only if the certificate from the client matches this profile. If you set the **Allow Authentication with User Credentials OR Client Certificate** option to **No**, you must select a **Certificate Profile**. If you set the **Allow Authentication with User Credentials OR Client Certificate** option to **Yes**, the **Certificate Profile** is optional. The certificate profile is independent of the OS. Also, this profile is active even if you enable Authentication Override, which overrides the Authentication Profile to allow authentication using encrypted cookies.

GlobalProtect Portals Portal Data Collection Tab

Select **Network** > **GlobalProtect** > **Portals** > **<portal-config>** > **Portal Data Collection** to define the data that the GlobalProtect app collects from endpoints and sends in the config selection criteria data after users successfully log in to the portal.

GlobalProtect Portal Data Collection Settings	Description
Certificate Profile	Select the certificate profile that the GlobalProtect portal uses to match the machine certificate sent by the GlobalProtect app.
Custom Checks	Define custom host information that you want the app to collect: • **Windows**—**Add** a check for a particular registry key or key value. • **Mac**—**Add** a check for a particular plist key or key value.

GlobalProtect Portals Agent Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Agent**

Select the **Agent** tab to define the agent configuration settings. The GlobalProtect portal deploys the configuration to the device after the connection is first established.

You can also specify that the portal automatically deploy trusted root certificate authority (CA) certificates and intermediate certificates. If the endpoints do not trust the server certificates that the GlobalProtect gateways and GlobalProtect Mobile Security Manager are using, the endpoints need these certificates to establish HTTPS connections to the gateways or Mobile Security Manager. The portal pushes the certificates you specify here to the client along with the client configuration.

To add a trusted root CA certificate, **Add** an existing certificate or **Import** a new one. To install (transparently) the trusted root CA certificates that are required for SSL Forward Proxy decryption in the certificate store on the client, select **Install in Local Root Certificate Store**.

Specify the trusted root CA certificate that the GlobalProtect app uses to verify the identity of the GlobalProtect portal and gateways. If the portal or gateway presents a certificate that has not been signed or issued by the same certificate authority that issued the trusted root CA, the GlobalProtect app cannot establish a connection with the portal or gateway.

If you have different types of users that require different configurations, you can create separate agent configurations to support them. The portal subsequently uses the user or group name and OS of the client to determine the agent configuration to deploy. As with security rule evaluations, the portal looks for a match, starting from the top of the list. When the portal finds a match, it delivers the corresponding configuration to the app. Therefore, if you have multiple agent configurations, it is important to order them so that more specific configurations (configurations for specific users or operating systems) are above the more generic configurations. Use **Move Up** and **Move Down** to reorder the configurations. As needed, **Add** a new agent configuration. For detailed information on configuring the portal and creating agent configurations, refer to GlobalProtect Portals in the GlobalProtect Administrator's Guide. When you **Add** a new agent configuration or modify an existing one, the **Configs** window opens and displays five tabs, which are described in the following tables:

- GlobalProtect Portals Agent Authentication Tab

- GlobalProtect Portals Agent Config Selection Criteria Tab
- GlobalProtect Portals Agent Internal Tab
- GlobalProtect Portals Agent External Tab
- GlobalProtect Portals Agent App Tab
- GlobalProtect Portals Agent HIP Data Collection Tab

GlobalProtect Portals Agent Authentication Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Agent** > *<agent-config>* > **Authentication**

Select the **Authentication** tab to configure the authentication settings that apply to the agent configuration.

GlobalProtect Portal Client Authentication Configuration Settings	Description
Authentication Tab	
Name	Enter a descriptive name for this configuration for client authentication.
Client Certificate	(Optional) Select the source that distributes the client certificate to an endpoint, which then presents the certificate to the gateways. A client certificate is required if you are configuring mutual SSL authentication. If SCEP is configured for pre-logon in the portal client configuration, the portal generates a machine certificate that is stored in the system certificate store for gateway authentication and connections. To use a certificate that is **Local** to the firewall instead of a generated certificate from the PKI through **SCEP**, select a certificate that is already uploaded to the firewall. If you use an internal CA to distribute certificates to endpoints, select **None** (default). When you select **None**, the portal does not push a certificate to the endpoint.
Save User Credentials	Select **Yes** to save the username and password on the app or select **No** to force the users to provide the password—either transparently via the endpoint or by manually entering one—each time they connect. Select **Save Username Only** to save only the username each time a user connects. Select **Only with User Fingerprint** to allow biometric sign-in. When biometric sign-on is enabled on an endpoint, GlobalProtect uses the saved user credentials when a finger-print scan matches a trusted finger-print template on the endpoint. *Don't save user credentials because it makes it easier for unauthorized users to gain access to sensitive resources and confidential information. Users should manually enter their credentials each time they connect to GlobalProtect.*

GlobalProtect Portal Client Authentication Configuration Settings	Description
Authentication Override	
Generate cookie for authentication override	Select this option to configure the portal to generate encrypted, endpoint-specific cookies. The portal sends this cookie to the endpoint after the user first authenticates with the portal.
Accept cookie for authentication override	Select this option to configure the portal to authenticate endpoints through a valid, encrypted cookie. When the endpoint presents a valid cookie, the portal verifies that the cookie was encrypted by the portal, decrypts the cookie, and then authenticates the user.
Cookie Lifetime	Specify the hours, days, or weeks that the cookie is valid. The typical lifetime is 24 hours. The ranges are 1–72 hours, 1–52 weeks, or 1–365 days. After the cookie expires, the user must enter login credentials and the portal subsequently encrypts a new cookie to send to the user endpoint.
Certificate to Encrypt/Decrypt Cookie	Select the certificate to use for encrypting and decrypting the cookie.  *Ensure that the portal and gateways use the same certificate to encrypt and decrypt cookies. (Configure the certificate as part of a gateway client configuration. See* Network > GlobalProtect > Gateways*).*
Components that Require Dynamic Passwords (Two-Factor Authentication)	
To configure GlobalProtect to support dynamic passwords—such as one-time passwords (OTPs)—specify the portal or gateway types that require users to enter dynamic passwords. Where two-factor authentication is not enabled, GlobalProtect uses regular authentication using login credentials (such as AD) and a certificate. When you enable a portal or a gateway type for two-factor authentication, that portal or gateway prompts the user after initial portal authentication to submit credentials and a second OTP (or other dynamic password). However, if you also enable authentication override, an encrypted cookie is used to authenticate the user (after the user is first authenticated for a new session) and, thus, preempts the requirement for the user to re-enter credentials (as long as the cookie is valid). Therefore, the user is transparently logged in whenever necessary as long as the cookie is valid. You specify the lifetime of the cookie.	
Portal	Select this option to use dynamic passwords to connect to the portal.
Internal gateways - all	Select this option to use dynamic passwords to connect to internal gateways.

GlobalProtect Portal Client Authentication Configuration Settings	Description
External gateways - manual only	Select this option to use dynamic passwords to connect to external gateways that are configured as **Manual** gateways.
External gateways-auto discovery	Select this option to use dynamic passwords to connect to any remaining external gateways that the app can automatically discover (gateways which are not configured as **Manual**).

GlobalProtect Portals Agent Config Selection Criteria Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Agent** > *<agent-config>* > **Config Selection Criteria**

Select the **Config Selection Criteria** tab to configure the matching criteria used to identify the endpoint type in deployments with both managed and unmanaged endpoints. The portal can push specified configurations to the endpoint based on the endpoint type.

GlobalProtect Portal Config Selection Criteria Settings	Description
User/User Group tab	
OS	**Add** one or more endpoint operating system (OS) to specify which endpoints receive this configuration. The portal automatically learns the OS of the endpoint and incorporates details for that OS in the client configuration. You can select **Any** OS or a specific OS (**Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows**, or **WindowsUWP**).
User/User Gruop	**Add** the specific users or user groups to which this configuration applies. *You must configure group mapping (Device > User Identification > Group Mapping Settings) before you can select user groups.* To deploy this configuration to all users, select **any** from the **User/User Group** drop-down. To deploy this configuration only to users with GlobalProtect apps in pre-logon mode, select **pre-logon** from the **User/User Group** drop-down.
Device Checks	
Machine account exists with device serial number	Configure matching criteria based on whether the endpoint serial number exists in the Active Directory.

GlobalProtect Portal Config Selection Criteria Settings	Description
Certificate Profile	Select the certificate profile that the GlobalProtect portal uses to match the machine certificate sent by the GlobalProtect app.
Custom Checks	
Custom Checks	Select this option to define custom host information to match.
Registry Key	To check Windows endpoints for a specific registry key, **Add** the **Registry Key** for which to match. To match only the endpoints that lack the specified registry key or key value, enable the **Key does not exist or match the specified value data** option. To match on specific values, **Add** the **Registry Value** and **Value Data**. To match endpoints that explicitly do not have the specified value or value data, select **Negate**.
Plist	To check macOS endpoints for a specific entry in the property list (plist), **Add** the **Plist** name. To match only the endpoints that do not have the specified plist, enable the **Plist does not exist** option. To match on specific key-value pairs within the plist, **Add** the **Key** and corresponding **Value**. To match endpoints that explicitly do not have the specified key or value, select **Negate**.

GlobalProtect Portals Agent Internal Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Agent** > *<agent-config>* > **Internal**

Select the **Internal** tab to configure the internal gateway settings for an agent configuration.

GlobalProtect Portal Internal Settings	Description
Internal Host Detection	
Internal Host Detection	Select this option to allow the GlobalProtect app to determine if it is inside the enterprise network. This option applies only to endpoints that are configured to communicate with internal gateways and is a best practice for these endpoints. When the user attempts to log in, the app does a reverse DNS lookup of an internal host using the specified **Hostname** to the specified **IP Address**. The host serves as a reference point that is reachable if the endpoint is inside the enterprise network. If the app finds the host, the endpoint is inside the network and the app connects to an internal gateway; if the app fails

GlobalProtect Portal Internal Settings	Description
	to find the internal host, the endpoint is outside the network and the app establishes a tunnel to one of the external gateways. • The IP address type can be **IPv4** (IPv4 traffic only), **IPv6** (IPv6 traffic only), or both. Use **IPv4** and **IPv6** if your network supports dual stack configurations, where IPv4 and IPv6 run at the same time. • The IP address must be compatible with the IP address type. For example, 172.16.1.0 for IPv4 or 21DA:D3:0:2F3b for IPv6. • If you choose **IPv4** and **IPv6**, enter the appropriate IP address type for each.
Hostname	Enter the **Hostname** that resolves to the IP address within the internal network.
Internal Gateways	
Specify the internal gateways to which an app can request access and also provide HIP reports (if HIP is enabled in the GlobalProtect Portals Agent Data Collection Tab).	**Add** internal gateways that include the following information for each: • **Name**—A label of up to 31 characters to identify the gateway. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. • **Address**—The IP address or FQDN of the firewall interface for the gateway. This value must match the Common Name (CN) and SAN (if specified) in the gateway server certificate. For example, if you used an FQDN to generate the certificate, you must enter the FQDN here. • **Source Address**—A source address or address pool for endpoints. When users connect, GlobalProtect recognizes the source address of the device. Only the GlobalProtect apps with IP addresses that are included in the source address pool can authenticate with this gateway and send HIP reports. • **DHCP Option 43 Code** (Windows and Mac only)—DHCP sub-option codes for gateway selection. Specify one or more sub-option codes (in decimal). The GlobalProtect app reads the gateway address from values defined by the sub-option codes.

GlobalProtect Portals Agent External Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Agent** > *<agent-config>* > **External**

Select the **External** tab to configure the external gateway settings for an agent configuration.

GlobalProtect Portal External Settings	Description
Cutoff Time (sec)	Specify the number of seconds that an app waits for all of the available gateways to respond before it selects the best gateway. For subsequent connection requests, the app tries to connect to only those gateways that responded before the cutoff. A value of 0 means the app uses the **TCP Connection Timeout** in **AppConfigurations** in the **App** tab (range is 0 to 10; default is 5).

GlobalProtect Portal External Settings	Description
External Gateways	
Specify the list of firewalls to which apps can try to connect when establishing a tunnel while not on the corporate network.	**Add** external gateways that include the following information for each: • **Name**—A label of up to 31 characters to identify the gateway. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. • **Address**—The IP address or FQDN of the firewall interface where the gateway is configured. The value must match the CN (and SAN if specified) in the gateway server certificate. For example, if you used a FQDN to generate the certificate, you must also enter the FQDN here. • **Source Region**—Source region for endpoints. When users connect, GlobalProtect recognizes the endpoint region and only allows users to connect to gateways that are configured for that region. For gateway choices, source region is considered first, then gateway priority. • **Priority**—Select a value (**Highest**, **High**, **Medium**, **Low**, **Lowest**, or **Manual only**) to help the app determine which gateway to use. **Manual only** prevents the GlobalProtect app from attempting to connect to this gateway when **Auto Discovery** is enabled on the endpoint. The app will first contact all specified gateways with a **Highest**, **High**, or **Medium** priority and establish a tunnel with the gateway that provides the fastest response. If the higher priority gateways are unreachable, the app next contacts any additional gateways with lower priority values (excludes **Manual only** gateways). • **Manual**—Select this option to let users manually select (or switch to) a gateway. The GlobalProtect app can connect to any external gateway that is configured as **Manual**. When the app pconnects to another gateway, the existing tunnel is disconnected and a new tunnel established. The manual gateways can also have a different authentication mechanism than the primary gateway. If an endpoint is restarted or if a rediscovery is performed, the GlobalProtect app connects to the primary gateway. This feature is useful if a group of users needs to connect temporarily to a specific gateway to access a secure segment of your network.
Third Party VPN	
Third Party VPN	To direct the GlobalProtect app to ignore selected, third-party VPN clients so that GlobalProtect does not conflict with them, **Add** the name of the VPN client: Select the name from the list, or enter the name in the field provided. GlobalProtect ignores the route settings for the specified VPN clients if you configure this feature.

GlobalProtect Portals Agent App Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Agent** > *<agent-config>* > **App**

Select the **App** tab to specify how end users interact with the GlobalProtect apps installed on their systems. You can define different app settings for the different GlobalProtect agent configurations you create. See the GlobalProtect Administrator's Guide to learn more about the latest updates on the GlobalProtect App Customization settings.

GlobalProtect App Configuration Settings	Description
Welcome Page	Select a welcome page to present to end-users after they connect to GlobalProtect. You can select the **factory-default** page or **Import** a custom page. The default is **None**.
App Configurations	
Connect Method	• **On-demand (Manual user initiated connection)**—Users must launch the GlobalProtect app, and then initiate a connection to the portal and enter their GlobalProtect credentials. This option is used primarily for remote access connections. • **User-logon (Always On)**—The GlobalProtect app automatically establishes a connection to the portal after the user logs in to an endpoint. The portal responds by providing the app with the appropriate agent configuration. Subsequently, the app sets up a tunnel to one of the gateways specified in the agent configuration received from the portal. • **Pre-logon**—Pre-logon ensures remote Windows and Mac users are always connected to the corporate network and enables user logon scripts and application of domain policies when the user logs in to the endpoint. Because the endpoint can connect to the corporate network as if it were internal, users can log in with new passwords when their passwords expire or receive help with password recovery if they forget their password. With pre-logon, the GlobalProtect app establishes a VPN tunnel to a GlobalProtect gateway before the user logs in to the endpoint; the endpoint requests authentication by submitting a pre-installed machine certificate to the gateway. Then, on Windows endpoints, the gateway reassigns the VPN tunnel from the pre-logon user to the username that logged in to the endpoint; on Mac endpoints, the app disconnects and creates a new VPN tunnel for the user. There are two pre-logon connect methods, either of which enables the same pre-logon functionality that takes place before users log in to the endpoint. However, after users log in to the endpoint, the pre-logon connect method determines when the GlobalProtect app connection is established: • **Pre-logon (Always On)**—The GlobalProtect a ppautomatically attempts to connect and reconnect to GlobalProtect gateways. Mobile devices do not support pre-logon functionality, and therefore will default to the **User-logon (Always On)** connect method if this connect method is specified. • **Pre-logon then On-demand**—Users must launch the GlobalProtect app, and then initiate the connection manually. Mobile devices do not support pre-logon

GlobalProtect App Configuration Settings	Description
	functionality, and therefore will default to the **On-demand (Manual user initiated connection)** connect method if this connect method is specified.
GlobalProtect App Config Refresh Interval (hours)	Specify the number of hours the GlobalProtect portal waits before it initiates the next refresh of an app'ss configuration (range is 1 to 168; default is 24).
Allow User to Disable GlobalProtect App	Specifies whether users are allowed to disable the GlobalProtect app and, if so, what—if anything—they must do before they can disable the app: • **Allow**—Allow any user to disable the GlobalProtect app as needed. • **Disallow**—Do not allow end users to disable the GlobalProtect app. • **Allow with Comment**—Allow users to disable the GlobalProtect app on their endpoint but require that they submit their reason for disabling the app. • **Allow with Passcode**—Allow users to enter a passcode to disable the GlobalProtect app. This option requires the user to enter and confirm a Passcode value that, like a password, does not display when typed. Typically, administrators provide a passcode to users before unplanned or unanticipated events prevent users from connecting to the network by using the GlobalProtect VPN. You can provide the passcode through email or as a posting on your organization's website. • **Allow with Ticket**—This option enables a challenge-response mechanism where, after a user attempts to disable GlobalProtect, the endpoint displays an 8-character hexadecimal ticket request number. The user must contact the firewall administrator or support team (preferably by phone for security purposes) to provide this number. From the firewall (**Network** > **GlobalProtect** > **Portals**), the administrator or support person can then click **Generate Ticket** and enter the ticket **Request** number to obtain the **Ticket** number (also an 8-character hexadecimal number). The administrator or support person provides this ticket number to the user, who then enters it into the challenge field to disable the app.
Allow User to Uninstall GlobalProtect App	Specifies whether users are allowed to uninstall the GlobalProtect app and, if so, what—if anything—they must do before they can uninstall the app: • **Allow**—Allow any user to uninstall the GlobalProtect app as needed. • **Disallow**—Do not allow end users to uninstall the GlobalProtect app. • **Allow with Password**—Enforce a password to uninstall the GlobalProtect app. This option requires the user to enter

GlobalProtect App Configuration Settings	Description
	and confirm a password before they can proceed with uninstallation. You can provide the password through email or as a posting on your organization's website. This option requires Content Release version 8196-5685 and later.
Allow User to Upgrade GlobalProtect App	Specifies whether end-users can upgrade the GlobalProtect app software and, if they can, whether they can choose when to upgrade: • **Disallow**—Prevent users from upgrading the app software. • **Allow Manually**—Allow users to manually check for and initiate upgrades by selecting **Check Version** in the GlobalProtect app. • **Allow with Prompt** (default)—Prompt users when a new version is activated on the firewall and allow users to upgrade their software when it is convenient. • **Allow Transparently**—Automatically upgrade the app software whenever a new version becomes available on the portal. • **Internal**—Automatically upgrade the app software whenever a new version becomes available on the portal, but wait until the endpoint is connected internally to the corporate network. This prevents delays caused by upgrades over low-bandwidth connections.
Allow User to Sign Out from GlobalProtect App (Windows, macOS, iOS, Android, and Chrome Only)	Specifies whether users are permitted to manually sign out of the Globalprotect app: • **Yes** (default)—Allow any user to sign out from the GlobalProtect app as needed. • **No**—Do not allow end users to sign out from the GlobalProtect app. This option requires Content Release version 8196-5685 and later.
Use Single Sign-on (Windows)	Select **No** to disable single sign-on (SSO). With SSO enabled (default), the GlobalProtect app automatically uses the Windows login credentials to authenticate and then connect to the GlobalProtect portal and gateway. GlobalProtect can also wrap third-party credentials to ensure that Windows users can authenticate and connect even when a third-party credential provider is used to wrap the Windows login credentials.
Use Single Sign-on (macOS)	Select **No** to disable single sign-on (SSO). With SSO enabled (default), the GlobalProtect app automatically uses the macOS login credentials to authenticate and then connect to the GlobalProtect portal and gateway.

GlobalProtect App Configuration Settings	Description
	This option requires Content Release version 8196-5685 and later.
Clear Single Sign-On Credentials on Logout (Windows Only)	Select **No** to keep single sign-on credentials when the user logs out. Select **Yes** (default) to clear them and force the user to enter credentials upon the next login.
Use Default Authentication on Kerberos Authentication Failure	Select **No** to use only Kerberos authentication. Select **Yes** (default) to retry authentication by using the default authentication method after a failure to authenticate with Kerberos. This feature is supported for Mac and Windows endpoints only.
Automatic Restoration of VPN Connection Timeout	Enter a timeout value, in minutes, from 0 to 180 to specify the action the GlobalProtect app takes when the tunnel is disconnected due to network instability or endpoint state changes by entering; default is 30. • 0—Disable this feature so that GlobalProtect does not attempt to reestablish the tunnel after the tunnel is disconnected. • 1-180—Enable this feature so that GlobalProtect attempts to reestablish the tunnel connection if the tunnel is down for a period of time which does not exceed the timeout value you specify here. For example, with a timeout value of 30 minutes, GlobalProtect does not attempt to reestablish the tunnel if the tunnel is disconnected for 45 minutes. However, if the tunnel is disconnected for 15 minutes, GlobalProtect attempts to reconnect because the number of minutes has not exceeded the timeout value.  *With Always-On VPN, if a user switches from an external network to an internal network before the timeout value expires, GlobalProtect does not perform network discovery. As a result, GlobalProtect reestablishes the tunnel to the last known external gateway. To trigger internal host detection, the user must select Rediscover Network from the GlobalProtect console.*
Wait Time Between VPN Connection Restore Attempts	Enter the amount of time, in seconds, the GlobalProtect app waits between attempts to reestablish the connection with the last-connected gateway when you enable **Automatic Restoration of VPN Connection Timeout**. Specify a longer or shorter wait time depending on your network conditions. Range is 1 to 60 seconds; the default is 5.
Enforce GlobalProtect Connection for Network Access	Select **Yes** to force all network traffic to traverse a GlobalProtect tunnel. Select **No** (default) if GlobalProtect is

GlobalProtect App Configuration Settings	Description
	not required for network access and users can still access the internet even when GlobalProtect is disabled or disconnected. To provide instructions to users before traffic is blocked, configure a **Traffic Blocking Notification Message** and optionally specify when to display the message (**Traffic Blocking Notification Delay**). To permit traffic required to establish a connection with a captive portal, specify a **Captive Portal Exception Timeout**. The user must authenticate with the portal before the timeout expires. To provide additional instructions, configure a **Captive Portal Detection Message** and optionally specify when to display the message (**Captive Portal Notification Delay**).  *In most cases, use the default selection No. Selecting Yes blocks all network traffic to and from the endpoint until the app connects to an internal gateway inside the enterprise or to an external gateway outside the enterprise network.*
Allow traffic to specified hosts/ networks when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established	If desired, you can configure up to ten IP addresses or network segments for which you want to allow access when you enforce GlobalProtect for network access but the connection is not established. Separate multiple values with commas. Exclusions can improve the user experience by allowing users to access local resources when GlobalProtect is disconnected. For example when GlobalProtect is not connected, GlobalProtect can exclude link-local addresses to allow access to a local network segment or broadcast domain.
Captive Portal Exception Timeout (sec)	To enforce GlobalProtect for network access but provide a grace period to allow users enough time to connect to a captive portal, specify the timeout in seconds (range is 0 to 3600). For example, a value of 60 means the user must log in to the captive portal within one minute after GlobalProtect detects the captive portal. A value of 0 means GlobalProtect does not allow users to connect to a captive portal and immediately blocks access.
Automatically Launch Webpage in Default Browser Upon Captive Portal Detection	To automatically launch your default web browser upon captive portal detection so that users can log in to the captive portal seamlessly, enter the fully qualified domain name (FQDN) or IP address of the website that you want to use for the initial connection attempt that initiates web traffic when the default web browser launches (maximum length is 256 characters). The captive portal then intercepts this website connection attempt and redirects the default web browser to the captive portal login page. If this field is empty (default), GlobalProtect does not launch the default web browser automatically upon captive portal detection.

GlobalProtect App Configuration Settings	Description
Traffic Blocking Notification Delay (sec)	Specify a value, in seconds, to determine when to display the notification message. GlobalProtect starts the countdown to display the notification after the network is reachable (range is 5 to 120; default is 15).
Display Traffic Blocking Notification Message	Specifies whether a message appears when GlobalProtect is required for network access. Select **No** to disable the message. Select **Yes** to enable the message (GlobalProtect displays the message when GlobalProtect is disconnected but detects that the network is reachable.)
Traffic Blocking Notification Message	Customize a notification message to display to users when GlobalProtect is required for network access. GlobalProtect displays the message when GlobalProtect is disconnected but detects the network is reachable. The message can indicate the reason for blocking the traffic and provide instructions on how to connect. For example: `To access the network, you much first connect to GlobalProtect.` The message must be 512 or fewer characters.
Allow User to Dismiss Traffic Blocking Notifications	Select **No** to always display traffic blocking notifications. By default the value is set to **Yes** meaning users are permitted to dismiss the notifications.
Display Captive Portal Detection Message	Specifies whether a message appears when GlobalProtect detects a captive portal. Select **Yes** to display the message. Select **No** (default) to suppress the message (GlobalProtect does not display a message when GlobalProtect detects a captive portal). *If you enable a Captive Portal Detection Message, the message appears 85 seconds before the Captive Portal Exception Timeout. So if the Capture Portal Exception Timeout is 90 seconds or less, the message appears 5 seconds after a captive portal is detected.*
Captive Portal Detection Message	Customize a notification message to display to users when GlobalProtect detects the network which provides additional instructions for connecting to a captive portal. For example: `GlobalProtect has temporarily permitted network access for you to connect to the internet. Follow instructions from your internet provider. If you let the connection time out, open GlobalProtect and click Connect to try again.`

GlobalProtect App Configuration Settings	Description
	The message must be 512 or fewer characters.
Captive Portal Detection Delay	If you enable a Captive Portal Detection Message, you can specify the delay in seconds after captive portal detection at which GlobalProtect displays the detection message (range is 1 to 120; default is 5).
Client Certificate Store Lookup	Select the type of certificate or certificates that an app looks up in its personal certificate store. The GlobalProtect app uses the certificate to authenticate to the portal or a gateway and then establish a VPN tunnel to the GlobalProtect gateway. • **User**—Authenticate by using the certificate that is local to the user's account. • **Machine**—Authenticate by using the certificate that is local to the endpoint. This certificate applies to all the user accounts permitted to use the endpoint. • **User and machine** (default)—Authenticate by using the user certificate and the machine certificate.
SCEP Certificate Renewal Period (days)	This mechanism is for renewing a SCEP-generated certificate before the certificate actually expires. You specify the maximum number of days before certificate expiry that the portal can request a new certificate from the SCEP server in your PKI system (range is 0 to 30; default is 7). A value of 0 means that the portal does not automatically renew the client certificate when it refreshes a client configuration. For an app to get the new certificate, the user must log in during the renewal period (the portal does not request the new certificate for a user during this renewal period unless the user logs in). For example, suppose that a client certificate has a lifespan of 90 days and this certificate renewal period is 7 days. If a user logs in during the final 7 days of the certificate lifespan, the portal generates the certificate and downloads it along with a refreshed client configuration. See GlobalProtect App Config Refresh Interval (hours).
Extended Key Usage OID for Client Certificate	Enter the extended key usage of a client certificate by specifying its object identifier (OID). This setting ensures that the GlobalProtect app selects only a certificate that is intended for client authentication and enables GlobalProtect to save the certificate for future use.
Retain Connection on Smart Card Removal (Windows Only)	Select **Yes** to retain the connection when a user removes a smart card containing a client certificate. Select **No** (default) to terminate the connection when a user removes a smart card.

GlobalProtect App Configuration Settings	Description
Allow Overriding Username from Client Certificate	Select **No** to force GlobalProtect to use the username of the client certificate and prevent GlobalProtect from overriding it (enabled by default).
Enable Advanced View	Select **No** to restrict the user interface on the app to the basic, minimum view (enabled by default).
Allow User to Dismiss Welcome Page	Select **No** to force the Welcome Page to appear each time a user initiates a connection. This restriction prevents a user from dismissing important information, such as terms and conditions that may be required by your organization to maintain compliance.
Enable Rediscover Network Option	Select **No** to prevent users from manually initiating a network rediscovery.
Enable Resubmit Host Profile Option	Select **No** to prevent users from manually triggering resubmission of the latest HIP.
Allow User to Change Portal Address	Select **No** to disable the **Portal** field on the **Home** tab in the GlobalProtect app. However, because the user will then be unable to specify a portal to which to connect, you must supply the default portal address in the Windows registry or Mac plist: • **Windows registry**—`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` with key `Portal` • **Mac plist**—`/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist` with key `Portal` For more information about pre-deploying the portal address, see Customizable App Settings in the GlobalProtect Administrator's Guide.
Allow User to Continue with Invalid Portal Server Certificate	Select **No** to prevent the app from establishing a connection with the portal if the portal certificate is not valid.
Display GlobalProtect Icon	Select **No** to hide the GlobalProtect icon on the endpoint. If the icon is hidden, users cannot perform certain tasks, such as viewing troubleshooting information, changing passwords, rediscovering the network, or performing an on-demand connection. However, HIP notification messages, login prompts, and certificate dialogs do display when user interaction is necessary.
User Switch Tunnel Rename Timeout (sec) (Windows only)	Specify the number of seconds that a remote user has to be authenticated by a GlobalProtect gateway after logging into an endpoint by using Microsoft's Remote Desktop Protocol (RDP) (range is 0 to 600; default is 0). Requiring the remote

GlobalProtect App Configuration Settings	Description
	user to authenticate within a limited amount of time maintains security. After authenticating the new user and switching the tunnel to the user, the gateway renames the tunnel. A value of 0 means that the current user's tunnel is not renamed but, instead, is immediately terminated. In this case, the remote user gets a new tunnel and has no time limit for authenticating to a gateway (other than the configured TCP timeout).
Pre-Logon Tunnel Rename Timeout (sec) (Windows Only)	This setting controls how GlobalProtect handles the pre-logon tunnel that connects an endpoint to the gateway. A value of -1 means the pre-logon tunnel does not time out after a user logs on to the endpoint; GlobalProtect renames the tunnel to reassign it to the user. However, the tunnel persists even if the renaming fails or if the user does not log in to the GlobalProtect gateway. A value of 0 means when the user logs on to the endpoint, GlobalProtect immediately terminates the pre-logon tunnel instead of renaming it. In this case, GlobalProtect initiates a new tunnel for the user instead of allowing the user to connect over the pre-logon tunnel. Typically, this setting is most useful when you set the **Connect Method** to **Pre-logon then On-demand**, which forces the user to manually initiate the connection after the initial logon. A value of 1 to 600 indicates the number of seconds in which the pre-logon tunnel can remain active after a user logs on to the endpoint. During this time, GlobalProtect enforces policies on the pre-logon tunnel. If the user authenticates with the GlobalProtect gateway within the timeout period, GlobalProtect reassigns the tunnel to the user. If the user does not authenticate with the GlobalProtect gateway before the timeout, GlobalProtect terminates the pre-logon tunnel.
Preserve Tunnel on User Logoff Timeout (sec)	To enable GlobalProtect to preserve the existing VPN tunnel after users log out of their endpoint, specify a **Preserve Tunnel on User Logoff Timeout** value (range is 0 to 600 seconds; default is 0 seconds). If you accept the default value of **0**, GlobalProtect does not preserve the tunnel following user logout.
Show System Tray Notifications (Windows only)	Select **No** to hide notifications from the user. Select **Yes** (default) to display notifications in the system tray area.
Custom Password Expiration Message (LDAP Authentication Only)	Create a custom message to display to users when their password is about to expire. The maximum message length is 200 characters.

GlobalProtect App Configuration Settings	Description
Automatically Use SSL When IPSec Is Unreliable (hours)	Specify the amount of time (in hours) during which you want the GlobalProtect app to **Automatically Use SSL When IPSec Is Unreliable** (range is 0-168 hours). If you configure this option, the GlobalProtect app does not attempt to establish an IPSec tunnel during the specified time period. This timer initiates each time an IPSec tunnel goes down due to a tunnel keepalive timeout. If you accept the default value of **0**, the app does not fall back to establishing an SSL tunnel if it can establish an IPSec tunnel successfully. It falls back to establishing an SSL tunnel only when the IPSec tunnel cannot be established.  *This option requires Content Release version _____ and later.*
GlobalProtect Connection MTU (bytes)	Enter the GlobalProtect connection maximum transmission unit (MTU) value between 1000 to 1420 bytes that is used by the GlobalProtect app to connect to the gateway. The default value is 1400 bytes. You can optimize the connection experience for end users connecting over networks that require MTU values lower than the standard of 1500 bytes. By reducing the MTU size, you can eliminate performance and connectivity issues that occur due to fragmentation when the VPN tunnel connections go through multiple Internet Service Providers (ISPs) and network paths with MTU lower than 1500 bytes.
Maximum Internal Gateway Connection Attempts	Enter the maximum number of times the GlobalProtect agent should retry the connection to an internal gateway after the first attempt fails (range is 0 to 100; default is 0, which means the GlobalProtect app does not retry the connection). By increasing the value, you enable the app to automatically connect to an internal gateway that is temporarily down or unreachable during the first connection attempt but comes back up before the specified number of retries are exhausted. Increasing the value also ensures that the internal gateway receives the most up-to-date user and host information.
Portal Connection Timeout (sec)	The number of seconds (between 1 and 600) before a connection request to the portal times out due to no response from the portal. When your firewall is running Applications and Threats content versions earlier than 777-4484, the default is 30. Starting with Content Release version 777-4484, the default is 5.
TCP Connection Timeout (sec)	The number of seconds (between 1 and 600) before a TCP connection request times out due to unresponsiveness from either end of the connection. When your firewall is running Applications and Threats content versions earlier than

GlobalProtect App Configuration Settings	Description
	777-4484, the default is 60. Starting with Content Release version 777-4484, the default is 5.
TCP Receive Timeout (sec)	The number of seconds before a TCP connection times out due to the absence of some partial response of a TCP request (range is 1 to 600; default is 30).
Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Windows Only)	(GlobalProtect 4.0.3 and later releases) Configure the DNS resolution preferences when the GlobalProtect tunnel is connected on Windows endpoints: • Select **Yes** (default) to enable the GlobalProtect app to allow Windows endpoints to resolve all DNS queries with the DNS servers you configure on the gateway instead of allowing the endpoint to send some DNS queries to the DNS servers set on the physical adapter. • Select **No** to allow Windows endpoints to send DNS queries to the DNS server set on the physical adapter if the initial query to the DNS server configured on the gateway is not resolved. This option retains the native Windows behavior to query all DNS servers on all adapters recursively but can result in long wait times to resolve some DNS queries. To configure DNS settings for GlobalProtect app 4.0.2 and earlier releases, use the **Update DNS Settings at Connect** option.
Update DNS Settings at Connect (Windows Only) (Deprecated)	(GlobalProtect 4.0.2 and earlier releases) Configure the DNS server preferences for the GlobalProtect tunnel: • Select **No** (default) to allow Windows endpoints to send DNS queries to the DNS server set on the physical adapter if the initial query to the DNS server configured on the gateway is not resolved. This option retains the native Windows behavior to query all DNS servers on all adapters recursively but can result in long wait times to resolve some DNS queries. • Select **Yes** to enable Windows endpoints to resolve all DNS queries with the DNS servers you configure on the gateway instead of the DNS servers set on the physical adapter on the endpoint. When you enable this option, GlobalProtect strictly enforces the gateway DNS settings and overrides the static settings for all physical adapters.  *When this setting is enabled, (set to Yes) GlobalProtect can fail to restore the previously saved DNS settings, and as a result, can prevent the endpoint from resolving DNS queries. This feature is deprecated and is replaced with an improved implementation so that this scenario does not occur. If you*

GlobalProtect App Configuration Settings	Description
	were previously using this feature we recommend upgrading to GlobalProtect app 4.0.3 or a later release. To configure DNS settings for GlobalProtect app 4.0.3 and later releases, use the **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel** option.
Detect Proxy for Each Connection (Windows only)	Select **No** to auto-detect the proxy for the portal connection and use that proxy for subsequent connections. Select **Yes** (default) to auto-detect the proxy at every connection.
Set Up Tunnel Over Proxy (Windows & Mac Only)	Specify whether GlobalProtect must use or bypass proxies. Select **No** to require GlobalProtect to bypass proxies. Select **Yes** to require GlobalProtect to use proxies. Based on the GlobalProtect proxy use, endpoint OS, and tunnel type, network traffic will behave differently.
Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows Only)	Select **No** to prevent the GlobalProtect app from sending HIP data when the status of the Windows Security Center (WSC) changes. Select **Yes** (default) to immediately send HIP data when the status of the WSC changes.
Enable Inbound Authentication Prompts from MFA Gateways	To support multi-factor authentication (MFA), a GlobalProtect endpoint must receive and acknowledge UDP prompts that are inbound from the gateway. Select **Yes** to enable a GlobalProtect endpoint to receive and acknowledge the prompt. Select **No** (default) for GlobalProtect to block UDP prompts from the gateway.
Network Port for Inbound Authentication Prompts (UDP)	Specifies the port number a GlobalProtect endpoint uses to receive inbound authentication prompts from MFA gateways. The default port is 4501. To change the port, specify a number from 1 to 65535.
Trusted MFA Gateways	Specifies the list of firewalls or authentication gateways a GlobalProtect endpoint trusts for multi-factor authentication. When a GlobalProtect endpoint receives a UDP message on the specified network port, GlobalProtect displays an authentication message only if the UDP prompt comes from a trusted gateway.
Inbound Authentication Message	Customize a notification message to display when users try to access a resource that requires additional authentication. When users try to access a resource that requires additional authentication, GlobalProtect receives a UDP packet containing the inbound authentication prompt and displays this message. The UDP packet also contains the URL for the Authentication Portal page you specify when you Configure Multi-Factor Authentication. GlobalProtect automatically appends the URL to the message. For example:

GlobalProtect App Configuration Settings	Description
	`You have attempted to access a protected resource that requires additional authentication. Proceed to authenticate at` The message must be 255 or fewer characters.
IPv6 Preferred	Specifies the preferred protocol for GlobalProtect endpoint communications. Select **No** to change the preferred protocol to IPv4.Select Yes (default) to make IPv6 the preferred connection a dual-stack environment.
Change Password Message	Customize a message to specify password policies or requirements when users change their active directory (AD) password. For example: `Passwords must contain at least one number and one uppercase letter.` The message must be 255 or fewer characters for two byte Unicode languages such as Chinese Simplified. For Japanese, the message must be 128 or fewer characters.
Log Gateway Selection Criteria	Select **Yes** to enable the GlobalProtect app to send the gateway selection criteria logs to the firewall. The default is **No**. The app does not send the enhanced logs for the gateway selection criteria to the firewall.
Display Status Panel at Startup (Windows Only)	Select **Yes** to automatically display the GlobalProtect status panel when users establish a connection for the first time. Select **No** to suppress the GlobalProtect status panel when users establish a connection for the first time.
Disable GlobalProtect App	
Passcode/Confirm Passcode	Enter and then confirm a passcode if the setting for **Allow User to Disable GlobalProtect App** is **Allow with Passcode**. Treat this passcode like a password—record it and store it in a secure place. You can distribute the passcode to new GlobalProtect users by email or post it in a support area of your company website. If circumstances prevent the endpoint from establishing a VPN connection and this feature is enabled, a user can enter this passcode in the app interface to disable the GlobalProtect app and get Internet access without using the VPN.
Max Times User Can Disable	Specify the maximum number of times that a user can disable GlobalProtect before the user must connect to a firewall. The default value of 0 means users have no limit to the number of times they can disable the app.

GlobalProtect App Configuration Settings	Description
Disable Timeout (min)	Specify the maximum number of minutes the GlobalProtect app can be disabled. After the specified time passes, the app tries to connect to the firewall. The default of 0 indicates that the disable period is unlimited. *Set a disable timeout value to restrict the amount of time for which users can disable the app. This ensures that GlobalProtect resumes and establishes the VPN when the timeout is over to secure the user and the user's access to resources.*
Mobile Security Manager Settings	
Mobile Security Manager	If you are using the GlobalProtect Mobile Security Manager for mobile device management (MDM), enter the IP address or FQDN of the device check#in (enrollment) interface on the GP-100 appliance.
Enrollment Port	The port number the mobile endpoint should use when connecting to the GlobalProtect Mobile Security Manager for enrollment. The Mobile Security Manager listens on port 443 by default. *Keep this port number so that mobile endpoint users are not prompted for a client certificate during the enrollment process (other possible values are 443, 7443, and 8443).*

GlobalProtect Portals Agent HIP Data Collection Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Agent** > *<agent-config>* > **HIP Data Collection**

Select the **HIP Data Collection** tab to define the data that the app collects from the endpoint in the HIP report:

GlobalProtect HIP Data Collection Configuration Settings	Description
Collect HIP Data	Clear this option to prevent the app from collecting and sending HIP data. *Enable GlobalProtect to collect HIP data for HIP-based policy enforcement, so the firewall can match HIP data from endpoints against the HIP objects and/or HIP profiles you define and then apply the appropriate policy.*

GlobalProtect HIP Data Collection Configuration Settings	Description
Max Wait Time (sec)	Specify how many seconds the app should search for HIP data before submitting the available data (range is 10-60; default is 20).
Certificate Profile	Select the certificate profile that the GlobalProtect portal uses to match the machine certificate sent by the GlobalProtect app.
Exclude Categories	Select **Exclude Categories** to specify the host information categories for which you do not want the app to collect HIP data. Select a **Category** (such as data-loss-prevention) to exclude from HIP collection. After selecting a category, you can **Add** a particular Vendor and, then, you can **Add** specific products from the vendor to further refine the exclusion as needed. Click **OK** to save settings in each dialog.
Custom Checks	Select **Custom Checks** to define custom host information you want the app to collect. For example, if you have any required applications that are not included in the Vendor or Product lists for creating HIP objects, you can create a custom check to determine whether that application is installed (it has a corresponding Windows registry or Mac plist key) or is currently running (has a corresponding running process): • **Windows**—**Add** a check for a particular registry key or key value. • **Mac**—**Add** a check for particular plist key or key value. • **Process List**—**Add** the processes you want to check for on user endpoints to see if they are running. For example, to determine whether a software application is running, add the name of the executable file to the process list. You can add a process to the **Windows** tab, the **Mac** tab, or both.

GlobalProtect Portals Clientless VPN Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Clientless VPN**

You can now configure the GlobalProtect portal to provide secure remote access to common enterprise web applications that use HTML, HTML5, and JavaScript technologies. Users have the advantage of secure access from SSL-enabled web browsers without installing GlobalProtect software. This is useful when you need to enable partner or contractor access to applications, and to safely enable unmanaged assets, including personal devices. This feature requires you to install a GlobalProtect subscription on the firewall that hosts the Clientless VPN from the GlobalProtect portal. Select the **Clientless VPN** tab to configure the GlobalProtect Clientless VPN settings on the portal as described in the following table.

GlobalProtect Portal Clientless Configuration Settings	Description
General tab	
Clientless VPN	Select **Clientless VPN** to specify general information about the Clientless VPN session:

GlobalProtect Portal Clientless Configuration Settings	Description
Hostname	The IP address or FQDN for the GlobalProtect portal that hosts the web applications landing page. The GlobalProtect Clientless VPN rewrites application URLs with this hostname. *If you use Network Address Translation (NAT) to provide access to the GlobalProtect portal, the IP address or FQDN you enter must match (or resolve to) the NAT IP address for the GlobalProtect portal (the public IP address).*
Security Zone	The zone for the Clientless VPN configuration. Security rules defined in this zone control which applications users can access.
DNS Proxy	The DNS server that resolves application names. Select a **DNS proxy** server or configure a **New DNS Proxy** (Network > DNS Proxy).
Login Lifetime	The number of **Minutes** (range is 60 to 1,440) or **Hours** (range is 1 to 24; default is 3) that a clientless SSL VPN session is valid. After the specified time, users must re-authenticate and start a new clientless VPN session.
Inactivity Timeout	The number of **Minutes** (range is 5 to 1,440; default is 30) or **Hours** (range is 1 to 24) that a clientless SSL VPN session can remain idle. If there is no user activity during the specified amount of time, the user must re-authenticate and start a new clientless VPN session.
Max User	The maximum numbers of users that can be logged into the portal at the same time (default is 10; range is 1 to no maximum). When the maximum number of users is reached, additional clientless VPN users cannot log in to the portal.
Applications tab	
Applications to User Mapping	**Add** one or more **Applications to User Mapping** to match users with published applications. This mapping controls which users or user groups can use a clientless VPN to access applications. You must define the applications and application groups before mapping them to users (Network > GlobalProtect > Clientless Apps and Network > GlobalProtect > Clientless App Groups). • **Name**—Enter a name for the mapping (up to 31 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores. • **Display application URL address bar**—Select this option to display an application URL address bar from which users can launch applications that are not published on the applications landing page. when enabled, users can click the **Application URL** link on the page and specify a URL.
User/User Group	You can **Add** individual users or user groups to which the current application configuration applies. These users have permission to launch the configured applications using a GlobalProtect clientless VPN.

GlobalProtect Portal Clientless Configuration Settings	Description
	You must configure group mapping (Device > User Identification > Group Mapping Settings) before you can select the groups. In addition to users and groups, you can specify when these settings apply to the users or groups: • **any**—The application configuration applies to all users (no need to **Add** users or user groups). • **select**—The application configuration applies only to users and user groups you **Add** to this list.
Applications	You can **Add** individual applications or application groups to the mapping. The **Source Users** you included in the configuration can use GlobalProtect clientless VPN to launch the applications you add.
Crypto Settings tab	
Protocol Versions	Select the required minimum and maximum TLS/SSL versions. The higher the TLS version, the more secure the connection. Choices include **SSLv3**, **TLSv1.0**, **TLSv1.1**, or **TLSv1.2**.
Key Exchange Algorithms	Select the supported algorithm types for key exchange. Choices include **RSA**, Diffie-Hellman (**DHE**), or Elliptic Curve Ephemeral Diffie-Hellman (**ECDHE**).
Encryption Algorithms	Select the supported encryption algorithms. **AES128** or higher is recommended.
Authentication Algorithms	Select the supported authentication algorithms. Choices are: **MD5**, **SHA1**, **SHA256**, or **SHA384**. **SHA256** or higher is recommended.
Server Certificate Verification	Enable which actions to take for the following issues that can occur when an application presents a server certificate: • **Block sessions with expired certificate**—If the server certificate has expired, block access to the application. • **Block sessions with untrusted issuers**—If the server certificate is issued from an untrusted certificate authority, block access to the application. • **Block sessions with unknown certificate status**—If the OCSP or CRL service returns a certificate revocation status of unknown, block access to the application. • **Block sessions on certificate status check timeout**—If the certificate status check times out before receiving a response from any certificate status service, block access to the application.
Proxy tab	
Name	A label of up to 31 characters to identify the proxy server that the GlobalProtect portal uses to access published applications. The name is case-

GlobalProtect Portal Clientless Configuration Settings	Description
	sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores.
Domains	Add the domains served by the proxy server.
Use Proxy	Select to allow the GlobalProtect portal to use the proxy server to access the published applications.
Server Port	Specify the hostname (or IP address) and port number of the proxy server.
User Password	Specify the username and password needed to log in to the proxy server. Enter the password again for verification.
Advanced Settings tab	
Rewrite Exclude Domain List	(Optional) **Add** domain names, host names, or IP addresses to the **Rewrite Exclude Domain List**. The clientless VPN acts as a reverse proxy and modifies pages returned by the published applications. When a remote users accesses the URL, the requests go through the GlobalProtect portal. In some cases, the application may have pages that do not need to be accessed through the portal. Specify domains that should be excluded from rewrite rules and cannot be rewritten. Paths are not supported in host and domain names. The wildcard character (*) for host and domain names can only appear at the beginning of the name (for example, *.etrade.com).

GlobalProtect Portal Satellite Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Satellite**

A satellite is a Palo Alto Networks® firewall—typically at a branch office—that acts as a GlobalProtect app to enable the satellite to establish VPN connectivity to a GlobalProtect gateway. Like a GlobalProtect app, a satellite receives its initial configuration from the portal, which includes the certificates and VPN configuration routing information and enable the satellite to connect to all configured gateways to establish VPN connectivity.

Before configuring the GlobalProtect satellite settings on the branch office firewall, you must configure an interface with WAN connectivity and set up a security zone and policy to allow the branch office LAN to communicate with the Internet. You can then select the **Satellite** tab to configure the GlobalProtect satellite settings on the portal as described in the following table.

GlobalProtect Portal Satellite Configuration Settings	Description
General	• **Name**—A name for this satellite configuration on the GlobalProtect portal.

GlobalProtect Portal Satellite Configuration Settings	Description
	• **Configuration Refresh Interval (hours)**—How often a satellite should check the portal for configuration updates (range is 1-48; default is 24).
Devices	**Add** a satellite using the firewall **Serial Number**. The portal can accept a serial number or login credentials to identify who is requesting a connection; if the portal does not receive a serial number, it requests login credentials. If you identify the satellite by its firewall serial number, you do not need to provide user login credentials when the satellite first connects to acquire the authentication certificate and its initial configuration. After the satellite authenticates by either a serial number or login credentials, the **Satellite Hostname** is automatically added to the portal.
Enrollment User/User Group	The portal can use **Enrollment User/User Group** settings with or without serial numbers to match a satellite to this configuration. Satellites that do not match on a serial number are required to authenticate either as an individual user or group member. **Add** the user or group you want to control with this configuration. *Before you can restrict the configuration to specific groups, you must enable Group Mapping in the firewall (Device > User Identification > Group Mapping Settings).*
Gateways	Click **Add** to enter the IP address or hostname of the gateway(s) satellites by which this configuration can establish IPSec tunnels. Enter the FQDN or IP address of the interface where the gateway is configured in the **Gateways** field. IP addresses can be specified as **IPv6**, **IPv4**, or both. Select **IPv6 Preferred** to specify preference of IPv6 connections in a dual stack environment. (Optional) If you are adding two or more gateways to the configuration, the **Routing Priority** helps the satellite pick the preferred gateway (range is 1 to 25). Lower numbers have higher priority (for gateways that are available). The satellite multiplies the routing priority by 10 to determine the routing metric. *Routes published by the gateway are installed on the satellite as static routes. The metric for the static route is 10 times the routing priority. If you have more than one gateway, be sure to set the routing priority so that routes advertised by backup gateways have higher metrics than the same routes advertised by primary gateways. For example, if you set the routing priority for the primary gateway and backup gateway to 1 and 10 respectively, the satellite will use 10 as the metric for the primary gateway and 100 as the metric for the backup gateway.* The satellite also shares its network and routing information with the gateways if you **Publish all static and connected routes to Gateway**

GlobalProtect Portal Satellite Configuration Settings	Description
	(**Network** > **IPSec tunnels** > **<tunnel** > **Advanced**—available only when you select **GlobalProtect Satellite on the <tunnel** > **General**).
Trusted Root CA	Click **Add** and then select the CA certificate for issuing gateway server certificates. Satellite Trusted Root CA certificates are pushed to endpoints at the same time as the portal agent configuration. *Specify a Trusted Root CA to verify gateway server certificates and establish secure VPN tunnel connections to GlobalProtect gateways. All your gateways should use the same issuer.* *You can Import or Generate a root CA certificate for issuing your gateway server certificates if one does not already exist on the portal.*
Client Certificate	
Local	• **Issuing Certificate**—Select the root CA issuing certificate the portal uses to issue certificates to a satellite after it successfully authenticates. If the needed certificate does not already exist on the firewall, you can **Import** or **Generate** it. *If a certificate does not already reside on the firewall, you can Import or Generate an issuing certificate.* • **OCSP Responder**—Select the OCSP Responder the satellite uses to verify the revocation status of certificates presented by the portal and gateways. Select **None** to specify that OCSP is not used for verifying revocation of a certificate. *Enable a satellite OCSP responder so that if a certificate was revoked, you are notified and can take appropriate action to establish a secure connection to the portal and gateways. To enable a satellite OCSP responder, you must also enable CRL and OCSP in the Certificate Revocation Checking settings (Device > Setup > Session > Decryption Settings).* • **Validity Period** (days)—Specify the GlobalProtect satellite certificate lifetime (range is 7 to 365; default is 7). • **Certificate Renewal Period** (days)—Specify the number of days before expiration that certificates can be automatically renewed (range is 3 to 30; default is 3).
SCEP	• **SCEP**—Select a SCEP profile for generating client certificates. If the profile is not in the drop-down, you can create a **New** profile. • **Certificate Renewal Period** (days)—Specify the number of days before expiration that certificates can be automatically renewed (range is 3 to 30; default is 3).

Network > GlobalProtect > Gateways

Select **Network** > **GlobalProtect** > **Gateways** to configure a GlobalProtect gateway. A gateway can provide VPN connections for GlobalProtect apps or for GlobalProtect satellites.

From the GlobalProtect Gateway dialog, **Add** a new gateway configuration or select an existing gateway configuration to modify it.

What are you looking for?	See:
What general settings can I configure for the GlobalProtect gateway?	GlobalProtect Gateways General Tab
How do I configure the gateway client authentication?	GlobalProtect Gateway Authentication Tab
How do I configure the tunnel and network settings that enable an app to establish a VPN tunnel with the gateway?	GlobalProtect Gateways Agent Tab
How do I configure the tunnel and network settings to enable the satellites to establish VPN connections with a gateway acting as a satellite?	GlobalProtect Gateway Satellite Tab
Looking for more?	For detailed, step-by-step instructions on setting up the portal, refer toConfigure GlobalProtect Gateways in the GlobalProtect Administrator's Guide.

GlobalProtect Gateways General Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **General**

Select the **General** tab to define the gateway interface to which the apps can connect and specify how the gateway authenticates endpoints.

GlobalProtect Gateway General Settings	Description
Name	Enter a name for the gateway (up to **31** characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in multiple virtual system mode, the **Location** is the virtual system (vsys) where the GlobalProtect gateway is available. For a firewall that is not in multi-vsys mode, the **Location** field does not appear in the GlobalProtect Gateway dialog.

GlobalProtect Gateway General Settings	Description
	After you save the gateway configuration, you cannot change the Location.
Network Settings Area	
Interface	Select the name of the firewall interface that will serve as the ingress interface for remote endpoints. (These interfaces must already exist.) *Do not attach an interface management profile that allows Telnet, SSH, HTTP, or HTTPS to an interface where you have configured a GlobalProtect portal or gateway because this will expose the management interface to the internet. Refer to Best Practices for Securing Administrative Access for more details on how to protect access to your management network.*
IP Address	(Optional) Specify the IP address for gateway access. Select the **IP Address Type**, then enter the **IP Address**. • The IP address type can be **IPv4** (IPv4 traffic only), **IPv6** (IPv6 traffic only), or **IPv4 and IPv6**. Use **IPv4 and IPv6** if your network supports dual-stack configurations, where IPv4 and IPv6 run at the same time. The IP address must be compatible with the IP address type. For example, 172.16.1.0 for IPv4 or 21DA:D3:0:2F3b for IPv6. If you choose **IPv4 and IPv6**, enter the appropriate address type for each.
Log Settings	
Log Successful SSL Handshake	(Optional) Creates detailed logs of successful SSL Decryption handshakes. Disabled by default. *Logs consume storage space. Before you log successful SSL handshakes, ensure you have the resources available to store the logs. Edit Device > Setup > Management > Logging and Reporting Settings to check the current log memory allocation to and re-allocate log memory among log types.*
Log Unsuccessful SSL Handshake	Creates detailed logs of unsuccessful SSL Decryption handshakes so you can find the cause of decryption issues. Enabled by default. *Logs consume storage space. To allocate more (or less) log storage space to Decryption logs, edit the log memory allocation (Device > Setup > Management > Logging and Reporting Settings).*
Log Forwarding	Specify the method and location to forward GlobalProtect SSL handshake (decryption) logs.

GlobalProtect Gateway Authentication Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **Authentication**

Select the **Authentication** tab to identify the SSL/TLS service profile and to configure the details of client authentication. You can add multiple client authentication configurations.

GlobalProtect Gateway Authentication Settings	
SSL/TLS Service Profile	Select an SSL/TLS service profile for securing this GlobalProtect gateway. For details about the contents of a service profile, see Device > Certificate Management > SSL/TLS Service Profile.
Client Authentication Area	
Name	Enter a unique name to identify this configuration.
OS	By default, the configuration applies to all endpoints. You can refine the list of endpoints by OS (**Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows**, or **WindowsUWP**), by **Satellite** devices, or by third-party IPSec VPN clients (**X-Auth**). The OS is the main differentiator between multiple configurations. If you need multiple configurations for one OS, you can further distinguish the configurations by your choice of authentication profile. *Order the configurations from most specific at the top of the list to most general at the bottom.*
Authentication Profile	Choose an authentication profile or sequence from the drop-down to authenticate access to the gateway. Refer to Device > Authentication Profile. *For client authentication, ensure that the Authentication Profile uses RADIUS or SAML with two-factor authentication. If you don't use RADIUS or SAML, then you need to configure a Certificate profile in addition to an Authentication Profile.*
Username Label	Specify a custom username label for GlobalProtect gateway login. For example, **Username (only)** or **Email Address (username@domain)**.
Password Label	Specify a custom password label for GlobalProtect gateway login. For example, **Password (Turkish)** or **Passcode** (for two-factor, token-based authentication).
Authentication Message	To help end users know what credentials they should use for logging into this gateway, you can enter a message or keep the

GlobalProtect Gateway Authentication Settings	
	default message. The message can have a maximum of 256 characters.
Allow Authentication with User Credentials OR Client Certificate	If you select **No**, users must authenticate to the gateway using both user credentials and client certificates. If you select **Yes**, users can authenticate to the gateway using either user credentials or client certificates.
Certificate Profile	
Certificate Profile	(Optional) Select the **Certificate Profile** the gateway uses to match those client certificates that come from user endpoints. With a Certificate Profile, the gateway authenticates the user only if the certificate from the client matches this profile. If you set the **Allow Authentication with User Credentials OR Client Certificate** option to **No**, you must select a **Certificate Profile**. If you set the **Allow Authentication with User Credentials OR Client Certificate** option to **Yes**, the **Certificate Profile** is optional. The certificate profile is independent of the OS.
Block login for quarantined devices	Specify whether to block gateway login for GlobalProtect client devices that are in the quarantine list (**Device** > **Device Quarantine**).

GlobalProtect Gateways Agent Tab

- **Network** > **GlobalProtect** > **Portals** > *<portal-config>* > **Agent**

Select the **Agent** tab to configure the tunnel settings that enable the app to establish a VPN tunnel with the gateway. In addition, this tab lets you specify timeouts for VPNs, network services of DNS and WINS, and HIP notification messages for end users upon matching or not matching a HIP profile attached to a Security policy rule.

Configure Agent settings on the following tabs:

- Tunnel Settings Tab
- Client Settings Tab
- Client IP Pool Tab
- Network Services Tab
- Connection Settings Tab
- Video Traffic Tab
- HIP Notification Tab

Tunnel Settings Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **Agent** > *<agent-config>* > **Tunnel Settings**

Select the **Tunnel Settings** tab to enable tunneling and configure the tunnel parameters.

Tunnel parameters are required if you are setting up an external gateway. If you are configuring an internal gateway, tunnel parameters are optional.

GlobalProtect Gateway Client Tunnel Mode Configuration Settings	Description
Tunnel Mode	Select **Tunnel Mode** to enable tunnel mode and then specify the following settings: • **Tunnel Interface**—Choose a tunnel interface for access to this gateway. • **Max User**—Specify the maximum number of users that can simultaneously access the gateway for authentication, HIP updates, and GlobalProtect app updates. If the maximum number of users is reached, subsequent users are denied access with a message that indicates the maximum number of users has been reached (range varies by platform and is displayed when the field is empty). • **Enable IPSec**—Select this option to enable IPSec mode for endpoint traffic, making IPSec the primary method and SSL-VPN the fallback method. The remaining options are not available until IPSec is enabled. • **GlobalProtect IPSec Crypto**—Select a GlobalProtect IPSec Crypto profile that specifies authentication and encryption algorithms for the VPN tunnels. The **default** profile uses AES-128-CBC encryption and SHA1 authentication. For details, see Network > Network Profiles > GlobalProtect IPSec Crypto. • **Enable X-Auth Support**—Select this option to enable Extended Authentication (X-Auth) support in the GlobalProtect gateway when IPSec is enabled. With X-Auth support, third party IPSec VPN clients that support X-Auth (such as the IPSec VPN client on Apple iOS and Android devices and the VPNC client on Linux) can establish a VPN tunnel with the GlobalProtect gateway. The X-Auth option provides remote access from the VPN client to a specific GlobalProtect gateway. Because X-Auth access provides limited GlobalProtect functionality, consider using the GlobalProtect App for simplified access to the full security feature set GlobalProtect provides on iOS and Android devices. Selecting **X-Auth Support** activates the **Group Name** and **Group Password** options: • If the group name and group password are specified, the first authentication phase requires both parties to use this credential to authenticate. The second phase requires a valid username and password, which is verified through the authentication profile configured in the Authentication section. • If no group name and group password are defined, the first authentication phase is based on a valid certificate presented by the third-party VPN client. This certificate is then validated through the certificate profile configured in the authentication section. • By default, the user is not required to re-authenticate when the key used to establish the IPSec tunnel expires. To require the user to re-authenticate, clear the **Skip Auth on IKE Rekey** option.

Client Settings Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **Agent** > *<agent-config>* > **Client Settings**

Select the **Client Settings** tab to configure settings for the virtual network adapter on the endpoint when the GlobalProtect app establishes a tunnel with the gateway.

Some Client Settings options are available only after you enable tunnel mode and define a tunnel interface on the Tunnel Settings Tab.

GlobalProtect Gateway Client Settings and Network Configuration	Description
Config Selection Criteria tab	
Name	Enter a name to identify the client settings configuration (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Source User	**Add** the specific users or user groups to which this configuration applies. *You must configure group mapping (Device > User Identification > Group Mapping Settings) before you can select users and groups.* To deploy this configuration to all users, select **any** from the **Source User** drop-down. To deploy this configuration only to users with GlobalProtect apps in pre-logon mode, select **pre-logon** from the **Source User** drop-down. *The client settings configuration is deployed to users only if the user matches the criteria for Source User, OS, AND Source Address.*
OS	To deploy this configuration based on the operating system of the endpoint, **Add** an OS (**Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows**, **WindowsUWP**). Alternatively, you can set this value to **Any** so that configuration deployment is based only on the user or user group and not on the operating system of the endpoint. *The client settings configuration is deployed to users only if the user matches the criteria for Source User, OS, AND Source Address.*
Source Address	To deploy this configuration based on user location, **Add** a source **Region** or local **IP Address** (IPv4 and IPv6). To deploy this configuration to all user locations, do not specify a **Region** or **IP Address**. You must also leave these fields empty if your users are running GlobalProtect app 4.0 and earlier releases, as this feature is not supported on older GlobalProtect app releases. *The Source Address match is successful if the location of a connecting user matches either the Region or the IP Address that you configure.*

GlobalProtect Gateway Client Settings and Network Configuration	Description
	The client settings configuration is deployed to users only if the user matches the criteria for Source User, OS, AND Source Address.
Authentication Override tab	
Authentication Override	Enable the gateway to use secure, device-specific, encrypted cookies to authenticate the user after the user first authenticates using the authentication scheme specified by the authentication or certificate profile. • **Generate cookie for authentication override**—During the lifetime of the cookie, the agent presents this cookie each time the user authenticates with the gateway. • **Cookie Lifetime**—Specify the hours, days, or weeks that the cookie is valid. The typical lifetime is 24 hours. The ranges are 1–72 hours, 1–52 weeks, or 1–365 days. After the cookie expires, the user must enter login credentials and the gateway subsequently encrypts a new cookie to send to user device. • **Accept cookie for authentication override**—Select this option to configure the gateway to accept authentication using the encrypted cookie. When the agent presents the cookie, the gateway validates that the cookie was encrypted by the gateway before authenticating the user. • **Certificate to Encrypt/Decrypt Cookie**—Select the certificate the gateway uses to use when encrypting and decrypting the cookie. *Ensure that the gateway and portal both use the same certificate to encrypt and decrypt cookies.*
IP Pools tab	
Retrieve Framed-IP-Address attribute from authentication server	Select this option to enable the GlobalProtect gateway to assign fixed IP addresses by use of an external authentication server. When this option is enabled, the GlobalProtect gateway allocates the IP address for connecting to devices by using the Framed-IP-Address attribute from the authentication server.
Authentication Server IP Pool	**Add** a subnet or range of IP addresses to assign to remote users. When the tunnel is established, the GlobalProtect gateway allocates the IP address in this range to connecting devices using the Framed-IP-Address attribute from the authentication server. You can add IPv4 addresses (such as 192.168.74.0/24 and 192.168.75.1-192.168.75.100) or IPv6 addresses (such as 2001:aa::1-2001:aa::10).

GlobalProtect Gateway Client Settings and Network Configuration	Description
	You can enable and configure **Authentication Server IP Pool** only if you enable **Retrieve Framed-IP-Address attribute from authentication server**. *The authentication server IP pool must be large enough to support all concurrent connections. IP address assignment is fixed and is retained after the user disconnects. Configure multiple ranges from different subnets to allow the system to offer clients an IP address that does not conflict with other interfaces on the client.* The servers and routers in the networks must route the traffic for this IP pool to the firewall. For example, for the 192.168.0.0/16 network, a remote user can receive the address 192.168.0.10.
IP Pool	**Add** a range of IP addresses to assign to remote users. When the tunnel is established, an interface is created on the remote user's endpoint with an address in this range. You can add IPv4 addresses (such as 192.168.74.0/24 and 192.168.75.1-192.168.75.100) or IPv6 addresses (such as 2001:aa::1-2001:aa::10). *To avoid conflicts, the IP pool must be large enough to support all concurrent connections. The gateway maintains an index of clients and IP addresses so that the client automatically receives the same IP address the next time it connects. Configuring multiple ranges from different subnets allows the system to offer clients an IP address that does not conflict with other interfaces on the client.* The servers and routers in the networks must route the traffic for this IP pool to the firewall. For example, for the 192.168.0.0/16 network, a remote user may be assigned the address 192.168.0.10.
Split Tunnel tab	
Access Route tab	
No direct access to local network	Select this option to disable split tunneling, including direct access to local networks on Windows and macOS endpoints. This function prevents a user from sending traffic to proxies or local resources, such as a home printer. When the tunnel is established, all traffic is routed through the tunnel and is subject to policy enforcement by the firewall.

GlobalProtect Gateway Client Settings and Network Configuration	Description
Include	**Add** routes to include in the VPN tunnel. These are the routes the gateway pushes to the remote users' endpoint to specify what user endpoints can send through the VPN connection. *To include all destination subnets or address objects, Include 0.0.0.0/0 and ::/0 as access routes.*
Exclude	**Add** routes to exclude from the VPN tunnel. These routes are sent through the physical adapter on endpoints rather than through the virtual adapter (the tunnel). You can define the routes you send through the VPN tunnel as routes you include in the tunnel, routes you exclude from the tunnel, or a combination of both. For example, you can set up split tunneling to allow remote users to access the internet without going through the VPN tunnel. Excluded routes should be more specific than the included routes to avoid excluding more traffic than you intend to exclude. If you don't include or exclude routes, every request is routed through the tunnel (no split tunneling). In this case, each internet request passes through the firewall and then out to the network. This method can prevent the possibility of an external party accessing user endpoints and gaining access to the internal network (with a user endpoint acting as a bridge).
Domain and Application tab	
Include Domain	Add the software as a service (SaaS) or public cloud applications that you want to include in the VPN tunnel using the domain and port (optional). These are the applications the gateway pushes to the remote users' endpoint to specify what user endpoints can send through the VPN connection. *You can configure a list of ports for each domain. If no ports are configured, all ports for the specified domain are subject to this policy.*
Exclude Domain	Add the software as a service (SaaS) or public cloud applications that you want to exclude from the VPN tunnel using the domain and port (optional). These applications are sent through the physical adapter on endpoints rather than the virtual adapter (the tunnel). *You can configure a list of ports for each domain. If no ports are configured, all ports for the specified domain are subject to this policy.* If you do not include or exclude any domains, every request is routed through the tunnel (no split tunneling). In this case,

GlobalProtect Gateway Client Settings and Network Configuration	Description
	each Internet request passes through the firewall and out to the network. This method can prevent external parties from accessing user endpoints to gain access to the internal network.
Include Client Application Process Name	Add the software as a service (SaaS) or public cloud applications that you want to include in the VPN tunnel using the application process name. These are the applications the gateway pushes to the endpoints of remote users to specify what those user endpoints can send through the VPN connection.
Exclude Client Application Process Name	Add the software as a service (SaaS) or public cloud applications that you want to exclude from the VPN tunnel using the application process name. These applications are sent through the physical adapter on endpoints rather than the virtual adapter (the tunnel). If you do not include or exclude any applications, every request is routed through the tunnel (no split tunneling). In this case, each Internet request passes through the firewall and out to the network. This method can prevent external parties from accessing user endpoints to gain access to the internal network.
Network Services tab	
DNS Server	Specify the IP address of the DNS server to which the GlobalProtect app with this client setting configuration sends DNS queries. You can add multiple DNS servers by separating each IP address with a comma.
DNS Suffix	Specify the DNS suffix that the endpoint should use locally when an unqualified hostname is entered that the endpoint cannot resolve. You can enter multiple DNS suffixes (up to 100) by separating each suffix with a comma.

Client IP Pool Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **Agent** > *<agent-config>* > **Client IP Pool**

Select the **Client IP Pool** tab to configure the global IP pool that is used to assign IPv4 or IPv6 addresses to all endpoints that connect to the GlobalProtect™ gateway.

GlobalProtect Gateway Client IP Pool Configuration Settings	Description
IP Pool	**Add** a range of IPv4 or IPv6 addresses to assign to remote users. After establishing the tunnel, the GlobalProtect gateway allocates IP addresses in

GlobalProtect Gateway Client IP Pool Configuration Settings	Description
	this range to all endpoints that connect through that tunnel. *If you configure IP pools at the gateway level (Network > GlobalProtect > Gateways > <gateway-config> > GlobalProtect Gateway Configuration > Agent > Client IP Pool), do not configure any IP pools at the client level (Network > GlobalProtect > Gateways > <gateway-config> > GlobalProtect Gateway Configuration > Agent > Client Settings > <client-setting> > Configs > IP Pools).*

Network Services Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **Agent** > *<agent-config>* > **Network Services**

Select the **Network Services** tab to configure DNS settings that will are assigned to the virtual network adapter on the endpoint when the GlobalProtect app establishes a tunnel with the gateway.

Network Services options are available only if you have enable tunnel mode and define a tunnel interface on the Tunnel Settings Tab.

GlobalProtect Gateway Client Network Services Configuration Settings	Description
Inheritance Source	Select a source to propagate DNS server and other settings from the selected DHCP client or PPPoE client interface into the GlobalProtect apps' configuration. With this setting, all client network configurations, such as DNS servers and WINS servers, are inherited from the configuration of the interface selected in the Inheritance Source.
Check inheritance source status	Click Inheritance Source to see the server settings that are currently assigned to the client interfaces.
Primary DNS Secondary DNS	Enter the IP addresses of the primary and secondary servers that provide DNS to the clients.
Primary WINS Secondary WINS	Enter the IP addresses of the primary and secondary servers that provide Windows Internet Naming Service (WINS) to the endpoints.
Inherit DNS Suffixes	Select this option to inherit the DNS suffixes from the inheritance source.

GlobalProtect Gateway Client Network Services Configuration Settings	Description
DNS Suffix	**Add** a suffix that the endpoint should use locally when an unqualified hostname, which it cannot resolve, is entered. You can enter multiple suffixes (up to 100) by separating each suffix with a comma.

Connection Settings Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **Agent** > *<agent-config>* > **Connection Settings**

Select the **Connection Settings** tab to define the timeout settings and authentication cookie usage restrictions for the GlobalProtect™ app.

GlobalProtect Gateway Client Tunnel Mode Connection Settings	Description
Timeout Configuration	
Login Lifetime	Specify the number of days, hours, or minutes allowed for a single gateway login session.
Inactivity Logout	Specify the number of days, hours, or minutes after which an inactive session is automatically logged out.
Disconnect on Idle	Specify the amount of time (in minutes) that passes before an endpoint is logged out of the GlobalProtect app after the app stops routing traffic through the VPN tunnel.
Authentication Cookie Usage Restrictions	
Disable Automatic Restoration of SSL VPN	Enable this option to prevent automatic restoration of SSL VPN tunnels. *If you enable this option, GlobalProtect will not support Resilient VPN.*
Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override) to	Enable this option to restrict authentication cookie usage based on one of the following conditions: • **The original Source IP for which the authentication cookie was issued**—Restricts authentication cookie usage to endpoints with the same public source IP address of the endpoint to which the cookie was originally issued. • **The original Source IP network range**—Restricts authentication cookie usage to endpoints with public source IP addresses within the designated network IP address range. Enter a **Source IPv4 Netmask** to specify a range of IPv4 addresses or enter a **Source IPv6 Netmask** to specify a range of IPv6 addresses.

GlobalProtect Gateway Client Tunnel Mode Connection Settings	Description
	If you set either netmask to **0**, this option is disabled for the specified IP address type. For example, you can set a netmask to **0** if your portal or gateway supports only one IP address type (IPv4 or IPv6) or if you want to enable this option for only one IP address type (when your portal or gateway supports both IPv4 and IPv6). You can set only one netmask to **0** in a given gateway configuration; you cannot simultaneously set both netmasks to **0**. If you accept the default **Source IPv4 Netmask** value of **32**, authentication cookie usage is restricted to the same public IPv4 address of the endpoint to which the cookie was originally issued. If you accept the default **Source IPv6 Netmask** value of **128**, authentication cookie usage is restricted to the same public IPv6 address of the endpoint to which the cookie was originally issued.

Video Traffic Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **Agent** > *<agent-config>* > **Video Traffic**

Select the **Video Traffic** tab to exclude video streaming traffic from the VPN tunnel.

GlobalProtect Gateway Video Traffic Configuration Settings	Description
Exclude video applications from the tunnel	Select this option to allow video streaming traffic to be excluded from the VPN tunnel.
Applications	**Add** or **Browse** for the video streaming applications that you want to exclude from the VPN tunnel. This video redirect is applicable to any video traffic type from the following applications: • Youtube • Dailymotion • Netflix For other video streaming applications, only the following video types can be redirected: • MP4 • WebM • MPEG Video streaming traffic can only be excluded from the VPN tunnel. If you do not exclude any video streaming applications, all requests are routed through the tunnel (no split tunneling). In this case, each Internet request passes through the firewall and out to the network. This method can

GlobalProtect Gateway Video Traffic Configuration Settings	Description
	prevent external parties from accessing user endpoints to gain access to the internal network.

HIP Notification Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **Agent** > *<agent-config>* > **HIP Notification**

Select the **HIP Notification** tab to define the notification messages that end users see when a security rule with a host information profile (HIP) is enforced.

These options are available only if you created HIP Profiles and added them to your security policies.

GlobalProtect Agent HIP Notification Configuration Settings	Description
HIP Notification	**Add** HIP Notifications and configure the options. You can **Enable** notifications for the **Match Message**, the **Not Match Message**, or both and then specify whether to **Show Notification As** a **System Tray Balloon** or a **Pop Up Message**. Then specify the message to match or not match. Use these settings to notify the end user about the state of the machine, such as a warning message that the host system does not have a required application installed. For the Match Message, you can also enable the option to **Include Mobile App List** to indicate what applications triggered the HIP match. *You can format HIP notification messages in rich HTML, which can include links to external web sites and resources. Click hyperlink ( ) in the rich text settings toolbar to add links.*

GlobalProtect Gateway Satellite Tab

- **Network** > **GlobalProtect** > **Gateways** > *<gateway-config>* > **Satellite**

A satellite is a Palo Alto Networks firewall—typically at a branch office—that acts as a GlobalProtect app to enable it to establish VPN connectivity to a GlobalProtect gateway. Select the **Satellite** tab to define the gateway tunnel and network settings to enable the satellites to establish VPN connections with it. You can also configure routes advertised by the satellites.

- Tunnel Settings tab
- Network Settings tab
- Route Filter tab

GlobalProtect Gateway Satellite Configuration Settings	Description
Tunnel Settings tab	
Tunnel Configuration	Select **Tunnel Configuration** and select an existing **Tunnel Interface**, or select **New Tunnel Interface** from the drop-down. See **Network > Interfaces > Tunnel** for more information. • **Replay attack detection**—Protect against replay attacks.  *Enable Replay attack detection to protect GlobalProtect satellites against replay attacks if you enable satellite tunnel configuration.* • **Copy TOS**—Copy the Type of Service (ToS) header from the inner IP header to the outer IP header of the encapsulated packets to preserve the original ToS information. • **Configuration refresh interval (hours)**—Specify how often satellites should check the portal for configuration updates (range is 1-48; default is 2).
Tunnel Monitoring	Select **Tunnel Monitoring** to enable the satellites to monitor gateway tunnel connections, allowing them to failover to a backup gateway if the connection fails. • **Destination Address**—Specify an **IPv4** or **IPv6** address for the tunnel monitor will use to determine if there is connectivity to the gateway (for example, an IP address on the network protected by the gateway). Alternatively, if you configured an IP address for the tunnel interface, you can leave this field blank and the tunnel monitor will instead use the tunnel interface to determine if the connection is active. • **Tunnel Monitor Profile**—**Failover** to another gateway is the only type of tunnel monitoring profile supported with LSVPN.  *Enable Tunnel Monitoring and configure a Tunnel Monitoring Profile to control the failover action if you enable satellite tunnel configuration.*
Crypto Profiles	Select an **IPSec Crypto Profile** or create a new one. A crypto profile determines the protocols and algorithms for identification, authentication, and encryption for the VPN tunnels. Because both tunnel endpoints in an LSVPN are trusted firewalls within your organization, you typically use the default profile, which uses ESP protocol, DH group2, AES 128 CVC encryption, and SHA-1 authentication. See Network > Network Profiles > GlobalProtect IPSec Crypto for more details.
Network Settings tab	
Inheritance Source	Select a source to propagate DNS server and other settings from the selected DHCP client or PPPoE client interface into the GlobalProtect satellite configuration. With this setting, all network configuration, such as DNS servers, are inherited from the configuration of the interface selected in the Inheritance Source.

GlobalProtect Gateway Satellite Configuration Settings	Description
Primary DNS Secondary DNS	Enter the IP addresses of the primary and secondary servers that provide DNS to the satellites.
DNS Suffix	Click **Add** to enter a suffix that the satellite should use locally when an unqualified hostname is entered that it cannot resolve. You can enter multiple suffixes by separating them with commas.
Inherit DNS Suffix	Select this option to send the DNS suffix to the satellites to use locally when an unqualified hostname is entered that it cannot resolve.
IP Pool	**Add** a range of IP addresses to assign to the tunnel interface on satellites upon establishment of the VPN tunnel. You can specify IPv6 or IPv4 addresses.  *The IP pool must be large enough to support all concurrent connections. IP address assignment is dynamic and not retained after the satellite disconnects. Configuring multiple ranges from different subnets will allow the system to offer satellites an IP address that does not conflict with other interfaces on the satellites.* The servers and routers in the networks must route the traffic for this IP pool to the firewall. For example, for the 192.168.0.0/16 network, a satellite can be assigned the address 192.168.0.10. If you are using dynamic routing, make sure that the IP address pool you designate for satellites does not overlap with the IP addresses you manually assigned to the tunnel interfaces on your gateways and satellites.
Access Route	Click **Add** and then enter routes as follows: • If you want to route all traffic from the satellites through the tunnel, leave this field blank. • To route only some traffic through the gateway (called split tunneling), specify the destination subnets that must be tunneled. In this case, the satellite routes traffic that is not destined for a specified access route by using its own routing table. For example, you can choose to tunnel only the traffic destined for your corporate network and use the local satellite to enable safe Internet access. • If you want to enable routing between satellites, enter the summary route for the network protected by each satellite.
Route Filter tab	
Accept published routes	Enable **Accept published routes** to accept routes advertised by the satellite into the gateway's routing table. If you do not select this option, the gateway does not accept any routes advertised by the satellites.
Permitted Subnets	If you want to be more restrictive about accepting the routes advertised by the satellites, **Add** Permitted subnets and define the subnets from which

GlobalProtect Gateway Satellite Configuration Settings	Description
	the gateway may accept routes; subnets advertised by the satellites that are not part of the list are filtered out. For example, if all the satellites are configured with 192.168.x.0/24 subnet on the LAN side, you can configure a permitted route of 192.168.0.0/16 on the gateway. This configuration causes the gateway to accept the routes from the satellite only if it is in the 192.168.0.0/16 subnet.

Network > GlobalProtect > MDM

If you are using a Mobile Security Manager to manage end user mobile endpoints and you are using HIP-enabled policy enforcement, you must configure the gateway to communicate with the Mobile Security Manager to retrieve the HIP reports for the managed endpoints.

Add MDM information for the Mobile Security Manager to enable the gateway to communicate with the Mobile Security Manager.

GlobalProtect MDM Settings	Description
Name	Enter a name for the Mobile Security Manager (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
	If the firewall is in multiple virtual system mode, the MDM settings displays the virtual system (vsys) where the Mobile Security Manager is available. For a firewall that is not in multi-vsys mode, this field does not appear in the MDM dialog. After you save the Mobile Security Manager, you cannot change its location.
Connection Settings	
Server	Enter the IP address or FQDN of the interface on the Mobile Security Manager where the gateway connects to retrieve HIP reports. Ensure that you have a service route to this interface.
Connection Port	The connection port is where the Mobile Security Manager listens for HIP report requests. The default port is 5008, which is the same port on which the GlobalProtect Mobile Security Manager listens. If you are using a third-party Mobile Security Manager, enter the port number on which that server listens for HIP report requests.
Client Certificate	Choose the client certificate for the gateway to present to the Mobile Security Manager when it establishes an HTTPS connection. This certificate is required only if the Mobile Security Manager is configured to use mutual authentication.
Trusted Root CA	Click **Add** and then select the root CA certificate that was used to issue the certificate for the interface where the gateway connects to retrieve HIP reports. (This server certificate can be different from the certificate issued for the endpoint check-in interface on the Mobile Security Manager).You must import the root CA certificate and add it to this list.

Network > GlobalProtect > Device Block List

Select **Network** > **GlobalProtect** > **Device Block List** (firewall only) to add endpoints to the GlobalProtect device block list. Endpoints on this list are not permitted to establish a GlobalProtect VPN connection.

Device Block List Settings	Description
Name	Enter a name for the device block list (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in multiple virtual system mode, the **Location** is the virtual system (vsys) where the GlobalProtect gateway is available. For a firewall that is not in multi-vsys mode, the **Location** field does not appear in the GlobalProtect Gateway dialog. After you save the gateway configuration, you cannot change the **Location**.
Host ID	Enter the unique ID that identifies the endpoint, a combination of host name and unique device ID. For each Host ID, specify the corresponding Hostname.
Hostname	Enter a hostname to identify the device (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

Network > GlobalProtect > Clientless Apps

Select **Network** > **GlobalProtect** > **Clientless Apps** to add applications that are accessible through the GlobalProtect Clientless VPN. You can add individual clientless applications and then select **Network** > **GlobalProtect** > **Clientless App Groups** to define application groups.

GlobalProtect Clientless VPN provides secure remote access to common enterprise web applications that use HTML, HTML5, and JavaScript technologies. Users have the advantage of secure access from SSL-enabled web browsers without installing GlobalProtect software. This is useful when you need to enable partner or contractor access to applications and to safely enable unmanaged assets, including personal devices.

You need the **GlobalProtect Clientless VPN** dynamic updates to use this feature. This feature also requires you to install a GlobalProtect subscription on the firewall that hosts the Clientless VPN from the GlobalProtect portal.

Clientless Apps Settings	Description
Name	Enter a descriptive name for the application (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in multiple virtual system mode, the **Location** is the virtual system (vsys) where the GlobalProtect gateway is available. For a firewall that is not in multi-vsys mode, the **Location** field does not appear in the GlobalProtect Gateway dialog. After you save the gateway configuration, you cannot change the **Location**.
Application Home URL	Enter the URL where the application is located (up to 4095 characters).
Application Description	(Optional) Enter a description of the application (up to 255 characters). Use only letters, numbers, spaces, hyphens, and underscores.
Application Icon	(Optional) Upload an icon to identify the application on the published application page. You can browse to upload the icon.

Network > GlobalProtect > Clientless App Groups

Select **Network** > **GlobalProtect** > **Clientless App Groups** to group applications that are accessible through the GlobalProtect Clientless VPN. You can add existing clientless applications to a group or configure new clientless applications for the group. Groups are useful for working with multiple applications at the same time. For example, you might have a standard set of SaaS applications (such as Workday, JIRA, or Bugzilla) that you want to configure for Clientless VPN access.

Clientless App Groups Settings	Description
Name	Enter a descriptive name for the application group (up to 31 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in multiple virtual system mode, the **Location** is the virtual system (vsys) where the GlobalProtect gateway is available. For a firewall that is not in multi-vsys mode, the **Location** field does not appear in the GlobalProtect Gateway dialog. After you save the gateway configuration, you cannot change the **Location**.
Applications	**Add** an **Application** from the drop-down or configure a new clientless application and add it to the group. To configure a new clientless application, refer to Network > GlobalProtect > Clientless Apps.

Objects > GlobalProtect > HIP Objects

Select **Objects** > **GlobalProtect** > **HIP Objects** to define objects for a host information profile (HIP). HIP objects provide the matching criteria for filtering the raw data reported by an app that you want to use to enforce policy. For example, if the raw host data includes information about several antivirus packages on an endpoint, you might be interested in a particular application because your organization requires that package. For this scenario, you create a HIP object to match the specific application you want to enforce.

The best way to determine the HIP objects you need is to determine how you will use the host information to enforce policy. Keep in mind that the HIP objects are merely building blocks that allow you to create the HIP profiles that your security policies can use. Therefore, you may want to keep your objects simple, matching on one thing, such as the presence of a particular type of required software, membership in a specific domain, or the presence of a specific endpoint OS. With this approach, you have the flexibility to create a very granular, HIP-augmented policy.

To create a HIP object, click **Add** to open the HIP Object dialog. For a description of what to enter in a specific field, see the tables that follow.

- HIP Objects General Tab
- HIP Objects Mobile Device Tab
- HIP Objects Patch Management Tab
- HIP Objects Firewall Tab
- HIP Objects Anti-Malware Tab
- HIP Objects Disk Backup Tab
- HIP Objects Disk Encryption Tab
- HIP Objects Data Loss Prevention Tab
- HIP Objects Certificate Tab
- HIP Objects Custom Checks Tab

For more detailed information on creating HIP-augmented security policies, refer to Configure HIP-Based Policy Enforcement in the *GlobalProtect Administrator's Guide*.

HIP Objects General Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **General**

Select the **General** tab to specify a name for the new HIP object and configure the object to match against general host information such as domain, operating system, or the type of network connectivity it has.

HIP Object General Settings	Description
Name	Enter a name for the HIP object (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	If you select **Shared**, the current HIP objects become available to: Every virtual system (vsys) on the firewall, if you are logged in to a firewall that is in multiple virtual system mode. If you clear this selection, the object will be available to only the vsys selected in the **Virtual System** drop-down of the **Objects** tab. For a firewall that is not in multi-vsys mode, this option is not available in the HIP Object dialog.

HIP Object General Settings	Description
	All device groups on Panorama™. If you clear this selection, the object will be available only to the device group selected in the **Device Group** drop-down of the **Objects** tab. After you save the object, you cannot change its **Shared** setting. Select **Objects** > **GlobalProtect** > **HIP Objects** to see the current **Location**.
Description	(Optional) Enter a description.
Host Info	Select this option to activate the options for configuring the host information.
Managed	Filter based on whether the endpoint is managed or not managed. To match endpoints that are managed, select **Yes**. To match endpoints that are not managed, select **No**.
Disable override (Panorama only)	Controls override access to the HIP object in the device groups that are descendants of the **Device Group** selected in the **Objects** tab. Select this option to prevent administrators from creating local copies of the object in descendant device groups by overriding its inherited values. This option is cleared by default (override is enabled).
Domain	To match on a domain name, choose an operator from the drop-down and enter a string to match.
OS	To match on a host OS, choose **Contains** from the first drop-down, select a vendor from the second drop-down, and then select an OS version from the third drop-down; or you can select **All** to match on any OS version from the selected vendor.
Client Version	To match on a specific version number, select an operator from the drop-down and then enter a string to match (or not match) in the text box.
Host Name	To match on a specific host name or part of a host name, select an operator from the drop-down and then enter a string to match (or not match, depending on what operator you selected) in the text box.
Host ID	The host ID is a unique ID that GlobalProtect assigns to identify the host. The host ID value varies by device type: • **Windows**—Machine GUID stored in the Windows registry (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid) • **macOS**—MAC address of the first built-in physical network interface • **Android**—Android ID • **iOS**—UDID • **Linux**—Product UUID retrieved from the system DMI table • **Chrome**—GlobalProtect-assigned unique alphanumeric string with length of 32 characters To match on a specific host ID, select the operator from the drop-down and then enter a string to match (or not match, depending on what operator you selected) in the text box.

HIP Object General Settings	Description
Serial Number	To match on all or part of an endpoint serial number, choose an operator from the drop-down and then enter a string to match.
Network	Use this field to enable filtering on a specific mobile device network configuration. This match criteria applies to mobile devices only. Select an operator from the drop-down and then select the type of network connection to filter on from the second drop-down: **Wifi**, **Mobile**, **Ethernet** (available only for **Is Not** filters), or **Unknown**. After you select a network type, enter any additional strings to match on, if available, such as the Mobile **Carrier** or Wifi **SSID**.

HIP Objects Mobile Device Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **Mobile Device**

Select the **Mobile Device** tab to enable HIP matching on data collected from mobile devices that run the GlobalProtect app.

To collect mobile device attributes and utilize them in HIP enforcement policies, GlobalProtect requires an MDM server. GlobalProtect currently supports HIP integration with the AirWatch MDM server.

HIP Object Mobile Device Settings	Description
Mobile Device	Select this option to enable filtering on host data collected from mobile devices that are running the GlobalProtect app and to enable the Device, Settings, and Apps tabs.
Device tab	• **Model**—To match on a particular device model, choose an operator from the drop-down and enter a string to match. • **Tag**—To match on tag value defined on the GlobalProtect Mobile Security Manager, choose an operator from the first drop-down and then select a tag from the second drop-down. • **Phone Number**—To match on all or part of a device phone number, choose an operator from the drop-down and enter a string to match. • **IMEI**—To match on all or part of a device International Mobile Equipment Identity (IMEI) number, choose an operator from the drop-down and enter a string to match.
Settings tab	• **Passcode**—Filter based on whether the device has a passcode set. To match devices that have a passcode set, select **Yes**. To match devices that do not have a passcode set, select no. • **Rooted/Jailbroken**—Filter based on whether the device has been rooted or jailbroken. To match devices that have been rooted or jailbroken, select **Yes**. To match devices that have not been rooted or jailbroken, select **No**. • **Disk Encryption**—Filter based on whether the device data has been encrypted. To match devices that have disk encryption enabled, select

HIP Object Mobile Device Settings	Description
	yes. To match devices that do not have disk encryption enabled, select no. • **Time Since Last Check-in**—Filter based on when the device last checked in with the MDM. Select an operator from the drop-down and then specify the number of days for the check-in window. For example, you could define the object to match devices that have not checked in within the last 5 days.
Apps tab	• **Apps**—(Android devices only) Select this option to enable filtering based on the apps that are installed on the device and whether or not the device has any malware-infected apps installed. • **Criteria** tab • **Has Malware**—Select **Yes** to match devices that have malware-infected apps installed. Select **No** to match devices that do not have malware-infected apps installed. Select **None** to not use **Has Malware** as match criteria. • **Include** tab • **Package**—To match devices that have specific apps installed, **Add** an app and enter the unique app name in reverse DNS format. For example, com.netflix.mediaclient and then enter the corresponding app **Hash**, which the GlobalProtect app calculates and submits with the device HIP report.

HIP Objects Patch Management Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **Patch Management**

Select the **Patch Management** tab to enable HIP matching on the patch status of the GlobalProtect endpoints.

HIP Object Patch Management Settings	Description
Patch Management	Select this option to enable matching on the patch management status of the host and enable the Criteria and Vendor tabs.
Criteria tab	Specify the following settings: • **Is Installed**—Match on whether patch management software is installed on the host. • **Is Enabled**—Match on whether patch management software is enabled on the host. If the **Is Installed** selection is cleared, this field is automatically set to **none** and is disabled for editing. • **Severity**—Select from the list of logical operators for matching on whether the host has missing patches of the specified severity value. Use the following mappings between the GlobalProtect severity values and the OPSWAT severity ratings to understand what each value means:

HIP Object Patch Management Settings	Description
	• **0**—Low • **1**—Moderate • **2**—Important • **3**—Critical • **Check**—Match on whether the endpoint has missing patches. • **Patches**—Match on whether the host has specific patches. Click **Add** and enter the KB article IDs for the specific patches to check for. For example, enter **3128031** to check for the Update for Microsoft Office 2010 (KB3128031) 32-Bit Edition.
Vendor tab	Define specific vendors of patch management software and products to look for on the endpoint to determine a match. Click **Add** and then choose a **Vendor** from the drop-down. Optionally, click Add to choose a specific **Product**. Click **OK** to save the settings.

HIP Objects Firewall Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **Firewall**

Select the **Firewall** tab to enable HIP matching based on the firewall software status of the GlobalProtect endpoints.

HIP Object Firewall Settings
Select **Firewall** to enable matching on the firewall software status of the host: • **Is Installed**—Match on whether firewall software is installed on the host. • **Is Enabled**—Match on whether firewall software is enabled on the host. If the **Is Installed** selection is cleared, this field is automatically set to **none** and is disabled for editing. • **Vendor and Product**—Define specific firewall software vendors and/or products to look for on the host to determine a match. Click **Add** and then choose a **Vendor** from the drop-down. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings. • **Exclude Vendor**—Select this option to match hosts that do not have software from the specified vendor.

HIP Objects Anti-Malware Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **Anti-Malware**

Select the **Anti-Malware** tab to enable HIP matching based on the antivirus or anti-spyware coverage on the GlobalProtect endpoints.

HIP Object Anti-Malware Settings
Select **Anti-Malware** to enable matching based on the antivirus or anti-spyware coverage on the host. Define additional matching criteria for the match as follows: • **Is Installed**—Match on whether antivirus or anti-spyware software is installed on the host.

HIP Object Anti-Malware Settings

- **Real Time Protection**—Match on whether real-time antivirus or anti-spyware protection is enabled on the host. If the **Is Installed** selection is cleared, this field is automatically set to **None** and is disabled for editing.
- **Virus Definition Version**—Match when the virus definitions have been updated within a specified number of days or release versions.
- **Product Version**—Match a specific version of the antivirus or anti-spyware software. To specify a version, select an operator from the drop-down, and then enter a string representing the product version.
- **Last Scan Time**—Specify whether to match based on the last time that the antivirus or anti-spyware scan was run. Select an operator from the drop-down, and then specify a number of **Days** or **Hours** to match against.
- **Vendor and Product**—Define specific antivirus or anti-spyware software vendors and/or products to look for on the host to determine a match. Click **Add**, and then choose a **Vendor** from the drop-down. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings.
- **Exclude Vendor**—Select this option to match hosts that do not have software from the specified vendor.

HIP Objects Disk Backup Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **Disk Backup**

Select the **Disk Backup** tab to enable HIP matching based on the disk backup status of the GlobalProtect endpoints.

HIP Object Disk Backup Settings

Select **Disk Backup** to enable matching on the disk backup status on the host and then define additional matching criteria for the match as follows:

- **Is Installed**—Match on whether disk backup software is installed on the host.
- **Last Backup Time**—Specify whether to match based on the time that the last disk backup was run. Select an operator from the drop-down and then specify a number of **Days** or **Hours** to match against.
- **Vendor and Product**—Define specific disk backup software vendors and products to match on the host. Click **Add** and then choose a **Vendor** from the drop-down. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings.
- **Exclude Vendor**—Select this option to match hosts that do not have software from the specified vendor.

HIP Objects Disk Encryption Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **Disk Encryption**

Select the **Disk Encryption** tab to enable HIP matching based on the disk encryption status of the GlobalProtect endpoints.

HIP Object Disk Encryption Settings	Description
Disk Encryption	Select **Disk Encryption** to enable matching on the disk encryption status on the host.
Criteria	Specify the following settings: • **Is Installed**—Match on whether disk encryption software is installed on the host. • **Encrypted Locations**—Click **Add** to specify the drive or path to check for disk encryption when determining a match: • **Encrypted Locations**—Enter specific locations to check for encryption on the host. • **State**—Specify how to match the state of the encrypted location by choosing an operator from the drop-down and then selecting a possible state (**full**, **none**, **partial**, **not-available**). Click **OK** to save the settings.
Vendor	Define specific disk encryption software vendors and products to match on the endpoint. Click **Add** and then choose a **Vendor** from the drop-down. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings and return to the **Disk Encryption** tab.

HIP Objects Data Loss Prevention Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **Data Loss Prevention**

Select the **Data Loss Prevention** tab to configure HIP matching that is based on whether the GlobalProtect endpoints are running data loss prevention software.

HIP Object Data Loss Prevention Settings
Select **Data Loss Prevention** to enable matching on the data loss prevention (DLP) status on the host (Windows hosts only) and then define additional matching criteria for the match as follows: • **Is Installed**—Match on whether DLP software is installed on the host. • **Is Enabled**—Match on whether DLP software is enabled on the host. If the **Is Installed** selection is cleared, this field is automatically set to **none** and is disabled for editing. • **Vendor and Product**—Define specific DLP software vendors and/or products to look for on the host to determine a match. Click **Add** and then choose a **Vendor** from the drop-down. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings. • **Exclude Vendor**—Select this option to match hosts that do not have software from the specified vendor.

HIP Objects Certificate Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **Certificate**

Select the **Certificate** tab to enable HIP matching based on the certificate profile and other certificate attributes.

HIP Object Certificate Settings
Select **Validate Certificate** to enable matching based on certificate profiles and certificate attributes. Then define the matching criteria as follows: • **Certificate Profile**—Select the certificate profile that the GlobalProtect gateway will use to validate the machine certificate sent in the HIP report. • **Certificate Field**—Select a certificate attribute used for matching against the machine certificate. • **Value**—Set the value for the attribute.

HIP Objects Custom Checks Tab

- **Objects** > **GlobalProtect** > **HIP Objects** > *<hip-object>* > **Custom Checks**

Select the **Custom Checks** tab to enable HIP matching on any custom checks you have defined on the GlobalProtect portal. For details on adding the custom checks to the HIP collection, see Network > GlobalProtect > Portals.

HIP Object Custom Checks Settings	Description
Custom Checks	Select **Custom Checks** to enable matching on custom checks you defined on the GlobalProtect portal.
Process List	To check the host system for a specific process, click **Add** and then enter the process name. By default, the app checks for running processes; if you want to see if a specific process is not running, clear the **Running** selection. Processes can be operating system level processes or user-space application processes.
Registry Key	To check Windows hosts for a specific registry key, click **Add** and enter the **Registry Key** to match. To match only the hosts that lack the specified registry key or the key's value, mark the **Key does not exist or match the specified value data** box. To match on specific values, click **Add** and then enter the **Registry Value** and **Value Data**. To match hosts that explicitly do not have the specified value or value data, select **Negate**. Click **OK** to save the settings.
Plist	To check Mac hosts for a specific entry in the property list (plist), click **Add** and enter the **Plist** name. To match only the hosts that do not have the specified plist, select **Plist does not exist**. To match on specific key-value pair within the plist, click **Add** and then enter the **Key** and the corresponding **Value** to match. To match hosts that explicitly do not have the specified key or value, select **Negate**. Click **OK** to save the settings.

Objects > GlobalProtect > HIP Profiles

Select **Objects** > **GlobalProtect** > **HIP Profiles** to create the HIP profiles—a collection of HIP objects to be evaluated together either for monitoring or for Security policy enforcement—that you use to set up HIP-enabled security policies. When creating HIP profiles, you can combine the HIP objects you previously created (as well as other HIP profiles) by using Boolean logic, so that when a traffic flow is evaluated against the resulting HIP profile, it will either match or not match. Upon a match, the corresponding policy rule is enforced; if there is no match, the flow is evaluated against the next rule (as with any other policy matching criteria).

To create a HIP profile, click **Add**. The following table provides information on what to enter in the fields in the HIP Profile dialog. For more detailed information on setting up GlobalProtect and the workflow for creating HIP-augmented security policies, refer to Configure HIP-Based Policy Enforcement in the *GlobalProtect Administrator's Guide*.

HIP Profile Settings	Description
Name	Enter a name for the profile (up to **31** characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	(Optional) Enter a description.
Shared	Select **Shared** to make the current HIP profile available to: • Every virtual system (vsys) on the firewall, if you are logged in to a firewall that is in multiple virtual system mode. If you clear this selection, the profile is available only to the vsys selected in the **Virtual System** drop-down on the **Objects** tab. For a firewall that is not in multi-vsys mode, this option does not appear in the HIP Profile dialog. • All device groups on Panorama. If you clear this selection, the profile is available only to the device group selected in the **Device Group** drop-down on the **Objects** tab. After you save the profile, you cannot change its **Shared** setting. Select **Objects** > **GlobalProtect** > **HIP Profiles** to view the current **Location**.
Disable override (Panorama only)	Controls override access to the HIP profile in device groups that are descendants of the **Device Group** selected in the **Objects** tab. Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This option is cleared by default (override is enabled).
Match	Click **Add Match Criteria** to open the HIP Objects/Profiles Builder. Select the first HIP object or profile you want to use as match criteria and then add (⊕) it to the **Match** text box on the HIP Objects/Profiles Builder dialog. Keep in mind that if you want the HIP profile to evaluate the object as a match only when the criteria in the object is not true for a flow, select **NOT** before adding the object. Continue adding match criteria as appropriate for the profile you are building, and ensure you select the appropriate Boolean operator (**AND**

HIP Profile Settings	Description
	or **OR**) between each addition (and using the **NOT** operator when appropriate). To create a complex Boolean expression, you must manually add the parenthesis in the proper places in the **Match** text box to ensure that the HIP profile is evaluated using the intended logic. For example, the following expression indicates that the HIP profile will match traffic from a host that has either FileVault disk encryption (Mac OS systems) or TrueCrypt disk encryption (Windows systems) and also belongs to the required Domain and has a Symantec antivirus client installed: `((“MacOS” and “FileVault”) or (“Windows” and “TrueCrypt”)) and “Domain” and “SymantecAV”` When you have finished adding the objects and profiles to the new HIP profile, click **OK**.

Device > GlobalProtect Client

The following topics describe how set up and manage the GlobalProtect app.

What are you looking for?	See:
View more information about the GlobalProtect software releases.	Managing the GlobalProtect Agent Software
Install the GlobalProtect software.	Setting Up the GlobalProtect Agent
Use the GlobalProtect software.	Using the GlobalProtect Agent
Looking for more?	For detailed, step-by-step instructions on setting up the GlobalProtect software, refer to Deploy the GlobalProtect App Software in the GlobalProtect Administrator's Guide.

Managing the GlobalProtect App Software

Select **Device** > **GlobalProtect Client** (firewall only) to download and activate the GlobalProtect app software on the firewall that hosts the portal. Thereafter, endpoints that connect to the portal download the app software. In the agent configurations you specify on the portal, you define how and when the portal pushes software to endpoints. Your configuration determines whether upgrades occur automatically when the app connects, whether end users are prompted to upgrade, or whether upgrading is prohibited for all or a particular set of users. See Allow User to Upgrade GlobalProtect App for more details. For details on the options for distributing the GlobalProtect app software and for step-by-step instructions for deploying the software, refer to Deploy the GlobalProtect App Software in the GlobalProtect Administrator's Guide.

For the initial download and installation of the GlobalProtect app, the user of the endpoint must be logged in with administrator rights. For subsequent upgrades, administrator rights are not required.

GlobalProtect Client Settings	Description
Version	This version number is of the GlobalProtect app software that is available on the Palo Alto Networks Update Server. To see if a new app software release is available from Palo Alto Networks, click **Check Now**. The firewall uses its service route to connect to the Update Server to determine if new versions are available and displays them at the top of the list.
Size	The size of the app software bundle.
Release Date	The date and time Palo Alto Networks made the release available.
Downloaded	A check mark in this column indicates that the corresponding version of the app software package has been downloaded to the firewall.
Currently Activated	A check mark in this column indicates that the corresponding version of the app software has package has been activated on the firewall and can be

GlobalProtect Client Settings	Description
	downloaded by connecting apps. Only one version of the software can be activated at a time.
Action	Indicates the current action you can take for the corresponding app software package as follows: • **Download**—The corresponding app software version is available on the Palo Alto Networks Update Server. Click **Download** to initiate the download. If the firewall does not have access to the Internet, use an Internet-connected computer to go to the Customer Support site, and then select **Updates** > **Software Updates** to look for and **Download** new app software versions to your local computer. Then manually **Upload** the app software to the firewall. • **Activate**—The corresponding app software version has been downloaded to the firewall, but apps cannot yet download it. Click **Activate** to activate the software and enable app upgrade. To activate a software update you manually uploaded to the firewall, click **Activate From File** and select the version you want to activate from the drop-down (you may need to refresh the screen for it to show as **Currently Activated**). • **Reactivate**—The corresponding app software has been activated and is ready for the endpoint to download. Because only one version of the GlobalProtect app software can be active on the firewall at one time, if your end users require access to a different version than is currently active, you have to **Activate** the other version to make it the **Currently Active** version.
Release Note	Provides a link to the GlobalProtect release notes for the corresponding app version.
☒	Remove the previously downloaded app software image from the firewall.

Setting Up the GlobalProtect App

The GlobalProtect app is an application that is installed on the endpoint (typically a laptop) to support GlobalProtect connections with portals and gateways. The app is supported by the GlobalProtect service (PanGP Service).

Make sure you select the correct installation option for your host operating system (32-bit or 64-bit). If you are installing on a 64-bit host, use the 64-bit browser and Java combination for the initial installation.

To install the app, open the installer file and follow the on-screen instructions.

Using the GlobalProtect App

The tabs in the **GlobalProtect Settings** panel, which opens when you launch the GlobalProtect app and select **Settings** from the **Settings** menu on the GlobalProtect status panel, contain useful information about status and settings and provide information to assist in troubleshooting connection issues.

- General tab—Displays the username and portal(s) associated with the GlobalProtect account. You can also add, delete, or modify portals from this tab.
- **Connection tab**—Displays the gateway(s) configured for the GlobalProtect app, and provides the following information about each gateway:
  - Gateway name
  - Tunnel status
  - Authentication status
  - Connection type
  - Gateway IP address or FQDN (only available in external mode)

  For internal mode, the Connection tab displays the entire list of available gateways. For external mode, the Connection tab displays the gateway to which you are connected and additional details about the gateway (such as gateway IP address and uptime).
- **Host Profile tab**—Displays the endpoint data that GlobalProtect uses to monitor and enforce security policies through the Host Information Profile (HIP). Click **Resubmit Host Profile** to manually resubmit HIP data to the gateway.
- **Troubleshooting tab**—On macOS endpoints, this tab allows you to **Collect Logs** and set the **Logging Level**. On Windows endpoints, this tab allows you to **Collect Logs**, set the **Logging Level**, and view the following information to assist in troubleshooting:
  - **Network Configurations**—Displays the current system configuration.
  - **Routing Table**—Displays information on how the GlobalProtect connection is currently routed.
  - **Sockets**—Displays socket information for the current active connections.
  - **Logs**—Allows the user to display logs for the GlobalProtect app and service. Choose the log type and debugging level. Click **Start** to begin logging and **Stop** to terminate logging.
- **Notification tab**—Displays the list of notifications triggered on the GlobalProtect app. To view more details about a specific notification, double-click the notification.

Panorama Web Interface

Panorama™ is the centralized management system for the Palo Alto Networks® family of next-generation firewalls. Panorama provides a single location from where you can oversee all applications, users, and content on your network and then use this knowledge to create policies that control and protect your network. Using Panorama for centralized policy and firewall management increases your operational efficiency as you manage your distributed firewall network. Panorama is available both as a dedicated hardware (M-Series) appliance and as a VMware virtual appliance (running on an ESXi server or the vCloud Air platform).

While many Panorama web interface views and settings are identical to those you see on the firewall web interface, the following topics describe options available exclusively on the Panorama web interface for managing Panorama, firewalls, and Log Collectors.

Looking for more?

See the Panorama Administrator's Guide for details on setting up and using Panorama for centralized management.

Use the Panorama Web Interface

The web interface on both Panorama and the firewall has the same look and feel. However, the Panorama web interface includes additional options and a Panorama-specific tab for managing Panorama and for using Panorama to manage firewalls and Log Collectors.

The following common fields appear in the header or footer of several Panorama web interface pages.

Common Field	Description
Context	You can use the **Context** drop-down above the left-side menu to switch between the Panorama web interface and a firewall web interface (see Context Switch).
	In the **Dashboard** and **Monitor** tabs, click refresh () in the tab header to manually refresh data in those tabs. You can also use the unlabeled drop-down on the right side of the tab header to select an automatic refresh interval in minutes (**1 min**, **2 mins**, or **5 mins**); to disable automatic refreshing, select **Manual**.
Access Domain	An access domain defines access to specific device groups, templates, and individual firewalls (through the **Context** drop-down). If you log in as an administrator with multiple access domains assigned to your account, the **Dashboard**, **ACC**, and **Monitor** tabs display information (such as log data) only for the **Access Domain** you select in the footer of the web interface.  *If only one access domain is assigned to your account, the web interface does not display the Access Domain drop-down.*
Device Group	A device group comprises firewalls and virtual systems that you manage as a group (see Panorama > Device Groups). The **Dashboard**, **ACC**, and **Monitor** tabs display information (such as log data) only for the **Device Group** you select in the tab header. In the **Policies** and **Objects** tabs, you can configure settings for a specific **Device Group** or for all device groups (select **Shared**).
Template	A template is a group of firewalls with common network and device settings, and a template stack is a combination of templates (see Panorama > Templates). In the **Network** and **Device** tabs, you configure settings for a specific **Template** or template stack. Because you can edit settings only within individual templates, the settings in these tabs are read-only if you select a template stack.
View by: Device Mode	By default, the **Network** and **Device** tabs display the settings and values available to firewalls that are in normal operational mode and that support multiple virtual systems and VPNs. However, you can use the following options to filter the tabs to display only the mode-specific settings you want to edit: • In the **Mode** drop-down, select or clear the **Multi VSYS**, **Operational Mode**, and **VPN Mode** options.

Common Field	Description
	• Set all the mode options to reflect the mode configuration of a particular firewall by selecting it in the **View by: Device** drop-down.

The **Panorama** tab provides the following pages for managing Panorama and Log Collectors.

Panorama Pages	Description
Setup	Select **Panorama** > **Setup** for the following tasks: • Specify general settings (such as the Panorama hostname) and settings for authentication, logs, reports, AutoFocus™, banners, the message of the day, and password complexity. These settings are similar to those you configure for firewalls: select Device > Setup > Management. • Back up and restore configurations, reboot Panorama, and shut down Panorama. These operations are similar to those you perform for firewalls: select Device > Setup > Operations. • Define server connections for DNS, NTP, and Palo Alto Networks updates. These settings are similar to those you configure for firewalls: select Device > Setup > Services. • Define network settings for Panorama interfaces. Select Panorama > Setup > Interfaces. • Specify settings for the WildFire™ appliance. These settings are similar to those you configure for firewalls: elect Device > Setup > WildFire. • Manage hardware security module (HSM) settings. These settings are similar to those you configure for firewalls: select Device > Setup > HSM.
High Availability	Enables you to configure high availability (HA) for a pair of Panorama management servers. Select Panorama > High Availability.
Config Audit	Enables you to see the differences between configuration files. Select Device > Config Audit.
Password Profiles	Enables you to define password profiles for Panorama administrators. Select Device > Password Profiles.
Administrators	Enables you to configure Panorama administrator accounts. Select Panorama > Administrators.  *If an administrator account is locked out, the Administrators page displays a lock in the Locked User column. You can click the lock to unlock the account.*
Admin Roles	Enables you to define administrative roles, which control the privileges and responsibilities of administrators who access Panorama. Select Panorama > Admin Roles.
Access Domain	Enables you to control administrator access to device groups, templates, template stacks, and the web interface of firewalls. Select Panorama > Access Domains.

Panorama Pages	Description
Authentication Profile	Enables you to specify a profile for authenticating access to Panorama. Select Device > Authentication Profile.
Authentication Sequence	Enables you to specify a series of authentication profiles to use for permitting access to Panorama. Select Device > Authentication Sequence.
User Identification	Enables you to configure a custom certificate profile for mutual authentication with User-ID agents. Select Device > User Identification > Connection Security.
Data Redistribution	Enables you to selectively redistribute data to other firewalls or Panorama management systems. Select Device > Data Redistribution.
Managed Devices	Enables you to manage firewalls, which includes adding firewalls to Panorama as *managed devices*, displaying firewall connection and license status, tagging firewalls, updating firewall software and content, and loading configuration backups. Select Panorama > Managed Devices > Summary.
Templates	Enables you to manage configuration options in the **Device** and **Network** tabs. Templates and template stacks enable you to reduce the administrative effort of deploying multiple firewalls with the same or similar configurations. Select Panorama > Templates.
Device Groups	Enables you to configure device groups, which group firewalls based on function, network segmentation, or geographic location. Device groups can include physical firewalls, virtual firewalls, and virtual systems. Typically, firewalls in a device group need similar policy configurations. Using the **Policies** and **Objects** tab on Panorama, device groups provide a way to implement a layered approach for managing policies across a network of managed firewalls. You can nest device groups in a tree hierarchy of up to four levels. Descendant groups automatically inherit the policies and objects of ancestor groups and of the Shared location. Select Panorama > Device Groups.
Managed Collectors	Enables you to manage Log Collectors. Because you use Panorama to configure Log Collectors, they are also called *managed collectors*. A managed collector can be local to the Panorama management server (M-Series appliance or Panorama virtual appliance in Panorama mode) or a Dedicated Log Collector (M-Series appliance in Log Collector mode). Select Panorama > Managed Collectors. You can also install Software Updates for Dedicated Log Collectors.  *You can* convert a Panorama management server to a DedicatedLogCollector.
Collector Groups	Enables you to manage Collector Groups. A Collector Group logically groups Log Collectors so you can apply the same configuration settings and assign firewalls to them. Panorama uniformly distributes the logs among all the disks in a Log Collector and across all members in the Collector Group. Select Panorama > Collector Groups.

Panorama Pages	Description
Plugins	Enables you to manage plugins for third-party integration, such as VMware NSX. Select Panorama > VMware NSX.
VMware NSX	Enables you to automate provisioning of VM-Series firewalls by enabling communication between the NSX Manager and Panorama. Select Panorama > VMware NSX.
Certificate Management	Enables you to configure and manage certificates, certificate profiles, and keys. Select Manage Firewall and Panorama Certificates.
Log Settings	Enables you to forward logs to Simple Network Management Protocol (SNMP) trap receivers, syslog servers, email servers, and HTTP servers. Select Device > Log Settings.
Server Profiles	Enables you to configure profiles for the different server types that provide services to Panorama. Select any of the following to configure a specific server type: • Device > Server Profiles > Email • Device > Server Profiles > HTTP • Device > Server Profiles > SNMP Trap • Device > Server Profiles > Syslog • Device > Server Profiles > RADIUS • Device > Server Profiles > TACACS+ • Device > Server Profiles > LDAP • Device > Server Profiles > Kerberos • Device > Server Profiles > SAML Identity Provider
Scheduled Config Export	Enables you to export Panorama and firewall configurations to an FTP server or Secure Copy (SCP) server on a daily basis. Select Panorama > Scheduled Config Export.
Software	Enables you to update Panorama software. Select Panorama > Software.
Dynamic Updates	Enables you to view the latest application definitions and information for new security threats, such as Antivirus signatures (threat prevention license required) and then update Panorama with the new definitions. Select Device > Dynamic Updates.
Support	Enables you to access product and security alerts from Palo Alto Networks. Select Device > Support.
Device Deployment	Enables you to deploy software and content updates to firewalls and Log Collectors. Select Panorama > Device Deployment.
Master Key and Diagnostics	Enables you to specify a master key to encrypt private keys on Panorama. By default, Panorama stores private keys in encrypted form even if you don't specify a new master key. Select Device > Master Key and Diagnostics.

Context Switch

In the header of every Panorama web interface page, you can use the **Context** drop-down above the left-side menu to switch between the Panorama web interface and a firewall web interface. When you select a firewall, the web interface refreshes to show all the pages and options for the selected firewall so that you can manage it locally. The drop-down displays only the firewalls to which you have administrative access (see Panorama > Access Domains) and that are connected to Panorama.

You can use the Filters to search for firewalls by Platforms (model), Device Groups, Templates, Tags, or HA Status. You can also enter a text string in the filter bar to search by Device Name.

The icons of firewalls that are in high availability (HA) mode will have colored backgrounds to indicate their HA state.

Panorama Commit Operations

Click **Commit** at the top right of the web interface and select an operation for pending changes to the Panorama configuration and changes that Panorama pushes to firewalls, Log Collectors, and WildFire clusters and appliances:

- **Commit** > **Commit to Panorama**—Activates changes you made in the configuration of the Panorama management server. This action also commits device group, template, Collector Group, and WildFire cluster and appliance changes to the Panorama configuration without pushing the changes to firewalls, Log Collectors, or WildFire clusters and appliances. Committing just to the Panorama configuration enables you to save changes that are not ready for activation on the firewalls, Log Collectors, or WildFire clusters and appliances.

  When pushing configurations to managed devices, Panorama 8.0 and later releases push the running configuration, which is the configuration that is committed to Panorama. Panorama 7.1 and earlier releases push the candidate configuration, which includes uncommitted changes. Therefore, Panorama 8.0 and later releases do not let you push changes to managed devices until you first commit the changes to Panorama.
- **Commit** > **Push to Devices**—Pushes the Panorama running configuration to device groups, templates, Collector Groups, and WildFire clusters and appliances.
- **Commit** > **Commit and Push**—Commits all configuration changes to the local Panorama configuration and then pushes the Panorama running configuration to device groups, templates, Collector Groups, and WildFire clusters and appliances.

You can filter pending changes by administrator or *location* and then commit, push, validate, or preview only those changes. The location can be specific device groups, templates, Collector Groups, Log Collectors, WildFire appliances and clusters, shared settings, or the Panorama management server.

When you commit changes, they become part of the running configuration. Changes that you haven't committed are part of the candidate configuration. Panorama queues commit requests so that you can initiate a new commit while a previous commit is in progress. Panorama performs the commits in the order they are initiated but prioritizes auto-commits that are initiated by Panorama (such as FQDN refreshes). However, if the queue already has the maximum number of administrator-initiated commits, you must wait for Panorama to finish processing a pending commit before initiating a new one. You can use the Task Manager (Tasks) to clear the commit queue or see details about commits. For more information on configuration changes, commit processes, commit validations, and the commit queue, refer to Panorama Commit and Validation Operations. You can also Save Candidate Configurations, Revert Changes, and import, export, or load configurations (Device > Setup > Operations).

The following options are available for committing, validating, or previewing configuration changes.

Field/Button	Description
The following options apply when you commit to Panorama by selecting **Commit** > **Commit to Panorama** or **Commit** > **Commit and Push**.	
Commit All Changes	Commits all changes for which you have administrative privileges (default). You cannot manually filter the scope of the configuration changes that Panorama commits when you select this option. Instead, the administrator role assigned to the account you used to log in determines the commit scope: • **Superuser role**—Panorama commits the changes of all administrators.

Field/Button	Description
	• **Custom role**—The privileges of the Admin Role profile assigned to your account determine the commit scope (see Panorama > Admin Roles). If the profile includes the privilege to **Commit For Other Admins**, Panorama commits changes configured by any and all administrators. If your Admin Role profile does not include the privilege to **Commit For Other Admins**, Panorama commits only your changes and not those of other administrators. If you have implemented access domains, Panorama automatically applies those domains to filter the commit scope (see Panorama > Access Domains). Regardless of your administrative role, Panorama commits only the configuration changes in the access domains assigned to your account.
Commit Changes Made By	Filters the scope of the configuration changes Panorama commits. The administrative role assigned to the account you used to log in determines your filtering options: • **Superuser role**—You can limit the commit scope to changes that specific administrators made and to changes in specific locations. • **Custom role**—The privileges of the Admin Role profile assigned to your account determine your filtering options (see Panorama > Admin Roles). If the profile includes the privilege to **Commit For Other Admins**, you can limit the commit scope to changes configured by specific administrators and to changes in specific locations. If your Admin Role profile does not include the privilege to **Commit For Other Admins**, you can limit the commit scope only to the changes you made in specific locations. Filter the commit scope as follows: • **Filter by administrator**—Even if your role allows committing the changes of other administrators, the commit scope includes only your changes by default. To add other administrators to the commit scope, click the *<usernames>* link, select the administrators, and click **OK**. • **Filter by location**—Select the specific locations for changes to Include in Commit. If you have implemented access domains, Panorama automatically filters the commit scope based on those domains (see Panorama > Access Domains). Regardless of your administrative role and your filtering choices, the commit scope includes only the configuration changes in the access domains assigned to your account. *After you load a configuration (Device > Setup > Operations), you must Commit All Changes.* When you commit changes to a device group, you must include the changes of all administrators who added, deleted, or repositioned rules for the same rulebase in that device group.
Commit Scope	Lists the locations that have changes to commit. Whether the list includes all changes or a subset of the changes depends on several

Field/Button	Description
	factors, as described for Commit All Changes and Commit Changes Made By. The locations can be any of the following: • **shared-object**—Settings that are defined in the Shared location. • *<device-group>*—The name of the device group in which the policy rules or objects are defined. • *<template>*—The name of the template or template stack in which the settings are defined. • *<log-collector-group>*—The name of the Collector Group in which the settings are defined. • *<log-collector>*—The name of the Log Collector in which the settings are defined. • *<wildfire-appliances>*—The serial number of the WildFire appliance in which the settings are defined. • *<wildfire-appliance-clusters>*—The name of the WildFire cluster in which the settings are defined.
Location Type	This column categorizes the locations of pending changes: • **Panorama**—Settings that are specific to the Panorama management server configuration. • **Device Group**—Settings that are defined in a specific device group. • **Template**—Settings that are defined in a specific template or template stack. • **Log Collector Group**—Settings that are specific to a Collector Group configuration. • **Log Collector**—Settings that are specific to a Log Collector configuration. • **WildFire Appliance Clusters**—Settings that are specific to a WildFire appliance cluster configuration. • **WildFire Appliances**—Settings that are specific to a WildFire appliance. • **Other Changes**—Settings that are not specific to any of the preceding configuration areas (such as shared objects).
Include in Commit (Partial commit only)	Enables you to select the changes you want to commit. By default, all changes within the **Commit Scope** are selected. This column displays only after you choose to **Commit Changes Made By** specific administrators. *There might be dependencies that affect the changes you include in a commit. For example, if you add an object and another administrator then edits that object, you cannot commit the change for the other administrator without also committing your own change.*
Group by Type	Groups the list of configuration changes in the **Commit Scope** by **Location Type**.

Field/Button	Description
Preview Changes	Enables you to compare the configurations you selected in the **Commit Scope** to the running configuration. The preview window uses color coding to indicate which changes are additions (green), modifications (yellow), or deletions (red). To help you match the changes to sections of the web interface, you can configure the preview window to display **Lines of Context** before and after each change. These lines are from the files of the candidate and running configurations that you are comparing.  *Because the preview results display in a new browser window, your browser must allow pop-ups. If the preview window does not open, refer to your browser documentation for the steps to allow pop-ups.*
Change Summary	Lists the individual settings for which you are committing changes. The **Change Summary** list displays the following information for each setting: • **Object Name**—The name that identifies the policy, object, network setting, or device setting. • **Type**—The type of setting (such as Address, Security rule, or Zone). • **Location Type**—Indicates whether the setting is defined in **Device Groups**, **Templates**, **Collector Groups**, **WildFire Appliances**, or **Wildfire Appliance Clusters**. • **Location**—The name of the device group, template, Collector Group, WildFire cluster, or WildFire appliance where the setting is defined. The column displays **Shared** for settings that are not defined in these locations. • **Operations**—Indicates every operation (create, edit, or delete) performed on the setting since the last commit. • **Owner**—The administrator who made the last change to the setting. • **Will Be Committed**—Indicates whether the commit will include the setting. • **Previous Owners**—Administrators who made changes to the setting before the last change. Optionally, you can **Group By** column name (such as **Type**).
Validate Commit	Validates whether the Panorama configuration has correct syntax and is semantically complete. The output includes the same errors and warnings that a commit would display, including rule shadowing and application dependency warnings. The validation process enables you to find and fix errors before you commit (it makes no changes to the running configuration). This is useful if you have a fixed commit window and want to be sure the commit will succeed without errors.
The following options apply when you push configuration changes to managed devices by selecting **Commit** > **Push to Devices** or **Commit** > **Commit and Push**.	

Field/Button	Description
Push Scope	Lists the locations that have changes to push. The locations that the scope includes by default depend on which of the following options you select: • **Commit** > **Commit and Push**—The scope includes all locations with changes that require a Panorama commit. • **Commit** > **Push to Devices**—The scope includes all locations associated with entities (firewalls, virtual systems, Log Collectors, WildFire clusters, WildFire appliances) that are `Out of Sync` with the Panorama running configuration (see Panorama > Managed Devices > Summary and Panorama > Managed Collectors for the synchronization status). For both selections, Panorama filters the **Push Scope** by: • **Administrators**—Panorama applies the same filters as for the **Commit Scope** (see Commit All Changes or Commit Changes Made By). • **Access domains**—If you implemented access domains, Panorama automatically filters the **Push Scope** based on those domains (see Panorama > Access Domains). Regardless of your administrative role and your filtering choices, the scope includes the configuration changes only in access domains assigned to your account. You can Edit Selections for the **Push Scope** instead of accepting the default locations.
Location Type	This column categorizes the locations of pending changes: • **Device Groups**—Settings defined in a specific device group. • **Templates**—Settings defined in a specific template or template stack. • **Log Collector Groups**—Settings specific to a Collector Group configuration. • **WildFire Clusters**—Settings specific to a WildFire cluster configuration. • **WildFire Appliances**—Settings specific to a WildFire appliance configuration.
Entities	For each device group or template, this column lists the firewalls (by device name or serial number) or virtual systems (by name) included in the push operation. *If you push changes to a Collector Group, the operation includes all the Log Collectors that are members of the group, even though they are not listed.*
Edit Selections	Click to select the entities to include in the push operation: • Device Groups and Templates • Log Collector Groups • WildFire Appliances and Clusters

Field/Button	Description
	Panorama won't let you push changes that you did not yet commit to the Panorama configuration.
Device Groups and Templates	**Edit Selections** and select **Device Groups** or **Templates** to display the options in the following rows.
Filters	Filter the list of templates, template stacks, or device groups and the associated firewalls and virtual systems. You can also filter managed firewalls according to their commit state, device state, tags, and high availability (HA) status.
Name	Select the templates, template stacks, device groups, firewalls, or virtual systems to include in the push operation.
Last Commit State	Indicates whether the firewall and virtual system configurations are synchronized with the template or device group configurations in Panorama.
HA Status	Indicates the high availability (HA) state of the listed firewalls: • **Active**—Normal traffic-handling operational state. • **Passive**—Normal backup state. • **Initiating**—The firewall is in this state for up to 60 seconds after bootup. • **Non-functional**—Error state. • **Suspended**—An administrator disabled the firewall. • **Tentative**—For a link or path monitoring event in an active/active configuration.
Changes Pending (Panorama) Commit	Indicates whether a Panorama commit is (yes) or is not (no) required before you push changes to the selected firewalls and virtual systems.
Preview Changes column	**Preview Changes** to compare the configurations you selected in the **Push Scope** to the Panorama running configuration. Panorama filters the output to show results only for the firewalls and virtual systems you selected in the **Device Groups** or **Templates** tab. The preview window uses color coding to indicate which changes are additions (green), modifications (yellow), or deletions (red). *Because the preview results display in a new browser window, your browser must allow pop-ups. If the preview window does not open, refer to your browser documentation for the steps to allow pop-ups.*
Select All	Selects all entries in the list.
Deselect All	Deselects all entries in the list.
Expand All	Displays the firewalls and virtual systems assigned to templates, template stacks, or device groups.

Field/Button	Description
Collapse All	Displays only the templates, template stacks, or device groups, not the firewalls or virtual systems assigned to them.
Group HA Peers	Groups firewalls that are peers in a high availability (HA) configuration. The resulting list displays the active firewall (or active-primary firewall in an active/active configuration) first and the passive firewall (or active-secondary firewall in an active/active configuration) in parentheses. This enables you to easily identify firewalls that are in HA mode. When pushing shared policies, you can push to the grouped pair instead of individual peers.  *For HA peers in an active/passive configuration, consider adding both firewalls or their virtual systems to the same device group, template, or template stack so that you can push the configuration to both peers simultaneously.*
Validate	Click to validate the configurations you are pushing to the selected firewalls and virtual systems. The Task Manager automatically opens to display the validation status.
Filter Selected	If you want the list to display only specific firewalls or virtual systems, select them and then select **Filter Selected**.
Merge with Candidate Config	(Selected by default) Merges the configuration changes pushed from Panorama with any pending configuration changes that administrators implemented locally on the target firewall. The push operation triggers PAN-OS® to commit the merged changes. If you clear this selection, the commit excludes the candidate configuration on the firewall.  *Clear this selection if you allow firewall administrators to commit changes locally on a firewall and you don't want to include those local changes when committing changes from Panorama.* Another best practice is to perform a configuration audit on the firewall to review any local changes before pushing changes from Panorama (see Device > Config Audit).
Include Device and Network Templates (Device Groups tab only)	(Selected by default) Pushes both the device group changes and the associated template changes to the selected firewalls and virtual systems in a single operation. To push these changes as separate operations, clear this option.
Force Template Values	(Disabled by default) Overrides all local configuration settings and removes all objects on the selected firewalls that don't exist in the template or template stack or that are overridden in the local configuration. The push operation reverts all existing configuration on the firewall and ensures that the firewall inherits only the settings defined in the template or template stack.

Field/Button	Description
	If you push a configuration with Force Template Values enabled, all overridden values on the firewall are replaced with values from the template. Before you use this option, check for overridden values on the firewalls to ensure your commit does not result in any unexpected network outages or issues caused by replacing those overridden values.
Log Collector Groups	**Edit Selections** and select **Log Collector Groups** to include in the push operation. This tab displays the following options: • **Select All**—Selects every Collector Group in the list. • **Deselect All**—Deselects every Collector Group in the list.
WildFire Appliances and Clusters	**Edit Selections** and select **WildFire Appliances and Clusters** to display the following options.
Filters	Filter the list of WildFire appliances and clusters.
Name	Select the WildFire appliances and clusters to which Panorama will push changes.
Last Commit State	Indicates whether the WildFire appliance and cluster configurations are synchronized with Panorama.
Remove Selections	Remove all firewalls listed in the Push Scope.
Validate Device Group Push	Validates the configurations you are pushing to the device groups in the Push Scope list. The Task Manager automatically opens to display the validation status.
Validate Template Push	Validates the configurations you are pushing to the templates in the Push Scope list. The Task Manager automatically opens to display the validation status.
Group by Location Type	Select to use **Location Type** to group the Push Scope list.
The following options apply when you commit the Panorama configuration or push changes to devices.	
Description	Enter a description (up to 512 characters) to help other administrators understand what changes you made. *The System log for a commit event will truncate descriptions longer than 512 characters.*
Commit / Push / Commit and Push	Starts the commit or, if other commits are pending, adds the commit request to the commit queue.

Defining Policies on Panorama

Device Groups on Panorama™ allow you to centrally manage firewall policies. You create policies on Panorama either as *Pre Rules* or *Post Rules*; Pre Rules and Post Rules allow you to create a layered approach for implementing policy.

You can define Pre rules and Post rules in a shared context, as shared policies for all managed firewalls, or in a device group context, to make the rules specific to a device group. Because you define Pre rules and Post Rules on Panorama and then push them from Panorama to the managed firewalls, you are able to view the rules on the managed firewalls but you can edit the Pre Rules and Post Rules only in Panorama.

- **Pre Rules**—Rules that are added to the top of the rule order and are evaluated first. You can use pre-rules to enforce the Acceptable Use Policy for an organization. For example, you can block access to specific URL categories or allow DNS traffic for all users.
- **Post Rules**—Rules that are added at the bottom of the rule order and are evaluated after the pre-rules and rules that are locally defined on the firewall. Post-rules typically include rules to deny access to traffic based on the App-ID™, User-ID™, or Service.
- **Default Rules**—Rules that specify how the firewall handles traffic that does not match any Pre Rules, Post Rules, or local firewall rules. These rules are part of the predefined Panorama configuration. To **Override** and enable editing of select settings in these rules, see Overriding or Reverting a Security Policy Rule.

Preview Rules to view a list of all rules before you push the rules to the managed firewalls. Within each rulebase, the hierarchy of rules is visually demarcated for each device group (and managed firewall) to make it easier to scan through a large numbers of rules.

When you add a new rule, static operational data for the rule are displayed. The universally unique identifier (UUID) column displays the 36-character UUID for the rule. The firewall generates the UUID on a per-rule basis. However, if you are pushing rules from Panorama, these rules have the same UUID, which is also displayed in the Combined Rules Preview. The **Created** column displays the time and date the rule was added to the rulebase. Additionally, the **Modified** column displays the time and date for the last time the rule was edited. If a policy rule was created before upgrading to PAN-OS 9.0, the **First Hit** data is used to establish the **Created** date. If no **First Hit** data is available for the rule, the time and date the firewall or Panorama management server was upgraded to PAN-OS 9.0 is used to establish the **Created** date.

When you add or edit a rule in Panorama, a **Target** tab displays. You can use this tab to apply the rule to specific firewalls or descendant device groups of the **Device Group** (or Shared location) where the rule is defined. In the **Target** tab, you can select **Any** (default), which means the rule applies to all the firewalls and descendant device groups. To target specific firewalls or device groups, deselect **Any** and select specific firewalls or device groups by name. To exclude specific firewalls or device groups, deselect **Any**, select the specific firewalls and device groups by name, and select **Target to all but these specified devices**. If the list of device groups and firewalls is long, you can apply Filters to search the entries by attributes (such as Platforms) or by a text string for matching names.

After you successfully add and push a rule in Panorama, **Rule Usage** displays whether the rule is Used by all devices in the device group, Partially Used by some devices in the device group, or Unused by devices in the device group. Panorama determines rule usage based on managed firewalls with Policy Rule Hit Count (enabled by default). In the Panorama context, you can view the rule usage for a Shared policy rule across all device groups. Additionally, you can change the context to an individual device group and view the total policy rule usage across all devices in the device group. **Preview Rules** will show the **Hit Count**, **Last Hit**, and **First Hit** for each policy rule for the device group. The total traffic hit count, as well as the first and last hits timestamps, persist through reboot, upgrade, and dataplane restart events. See Monitor Policy Rule Usage.

Group Rules by Tag to apply a tag that allows you to group like policy rules for better visualization of rule functions and provides easier management of policy rules across your rulebase. Rules grouped by tags show the list of tag groups, but maintain the rule priority listing. You can append rules to the end of a tag group,

move rules to a different tag group, apply additional tags to rules in a tag group, and filter or search using the group tag.

To track changes to policy rules, add an **Audit Comment** to describe the changes you make to and why a rule was created or modified. After you enter an audit comment is entered and configuration change is committed, the audit comment is preserved in the **Audit Comment Archive** where you can view all previous audit comments for the selected rule. You can search for the audit comment in Global Find. The Audit Comment Archive is read-only.

Administrative users who have access to the Policies tab can export the policy rules that are displayed on the web interface as **PDF/CSV**. See Export Configuration Table Data.

To create policies, see the relevant section for each rulebase:

- Policies > Security
- Policies > NAT
- Policies > QoS
- Policies > Policy Based Forwarding
- Policies > Decryption
- Policies > Application Override
- Policies > Authentication
- Policies > DoS Protection
- Policies > SD-WAN

Log Storage Partitions for a Panorama Virtual Appliance in Legacy Mode

- Panorama > Setup > Operations

By default, a Panorama virtual appliance in Legacy mode has a single disk partition for all data in which 10.89GB is allocated for log storage. Increasing disk size does not increase the log storage capacity; however, you can modify the log storage capacity using the following options:

- **Network File System (NFS)**—The option to mount NFS storage is available only for a Panorama virtual appliance that is in Legacy mode and running on a VMware ESXi server. To mount NFS storage, select **Storage Partition Setup** in the Miscellaneous section, set the **Storage Partition** to **NFS V3**, and configure the settings as described in Table: NFS Storage Settings.
- **Default internal storage**—Revert to the default internal storage partition (applicable only to Panorama on an ESXi server or on the vCloud Air platform where you previously configured another virtual logging disk or mounted to an NFS). To revert to the default internal storage partition, select **Storage Partition Setup** in the Miscellaneous section and set the **Storage Partition** to **Internal**.
- **Virtual logging disk**—You can add another virtual disk (up to 8TB) for Panorama running on VMware ESXi version 5.5 and later releases or for Panorama running on the VMware vCloud Air platform. However, Panorama stops using the default 10.89GB log storage on the original disk and copies any existing logs to the new disk. (Earlier ESXi versions support only up to 2TB virtual disks.)

You must reboot Panorama after changing the storage partition settings: select Panorama > Setup > Operations and Reboot Panorama.

NFS storage is not available to the Panorama virtual appliance in Panorama mode or to M-Series appliances.

Table 1: Table: NFS Storage Settings

Panorama Storage Partition Settings —NFS V3	Description
Server	Specify the FQDN or IP address of the NFS server.
Log Directory	Specify the full path name of the directory where the logs will reside.
Protocol	Specify the protocol (UDP or TCP) for communication with the NFS server.
Port	Specify the port for communication with the NFS server.
Read Size	Specify the maximum size in bytes (range is 256 to 32,768) for NFS read operations.
Write Size	Specify the maximum size in bytes (range is 256 to 32,768) for NFS write operations.
Copy on Setup	Select to mount the NFS partition and copy any existing logs to the destination directory on the server when Panorama boots.

Panorama Storage Partition Settings —NFS V3	Description
Test Logging Partitions	Select to perform a test that mounts the NFS partition and presents a success or failure message.

Panorama > Setup > Interfaces

- Panorama > Setup > Interfaces

Select **Panorama** > **Setup** > **Interfaces** to configure the interfaces that Panorama uses to manage firewalls and Log Collectors, deploy software and content updates to firewalls and Log Collectors, collect logs from firewalls, and communicate with Collector Groups. By default, Panorama uses the management (MGT) interface for all communication with firewalls and Log Collectors.

To reduce traffic on the MGT interface, configure other interfaces to deploy updates, collect logs, and communicate with Collector Groups. In an environment with heavy log traffic, you can configure several interfaces for log collection. Additionally, to improve the security of management traffic, you can define a separate subnet (IPv4 Netmask or IPv6 Prefix Length) for the MGT interface that is more private than the subnets for the other interfaces.

The available interfaces vary based on the Panorama model.

Interface	Maximum Speed	M-500 Appliance	Panorama Virtual Appliance
Management (MGT)	1Gbps	✓	✓
Ethernet1 (Eth1)	1Gbps	✓	—
Ethernet2 (Eth2)	1Gbps	✓	—
Ethernet3 (Eth3)	1Gbps	✓	—
Ethernet4 (Eth4)	10Gbps	✓	—
Ethernet5 (Eth5)	10Gbps	✓	—

To configure an interface, click the Interface Name and configure the settings described in the following table.

Always specify the IP address, the netmask (for IPv4) or prefix length (for IPv6), and the default gateway for the MGT interface. If you omit values for some settings (such as the default gateway), you can access Panorama only through the console port for future configuration changes. You cannot commit the configurations for other interfaces unless you specify all three settings.

Interface Settings	Description
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	You must enable an interface to configure it. The exception is the MGT interface, which is enabled by default.
IP Address (IPv4)	If your network uses IPv4 addresses, assign an IPv4 address to the interface.
Netmask (IPv4)	If you assigned an IPv4 address to the interface, you must also enter a network mask (such as 255.255.255.0).

Interface Settings	Description
Default Gateway (IPv4)	If you assigned an IPv4 address to the interface, you must also assign an IPv4 address to the default gateway (the gateway must be on the same subnet as the interface).
IPv6 Address/Prefix Length	If your network uses IPv6 addresses, assign an IPv6 address to the interface. To indicate the netmask, enter an IPv6 prefix length (such as 2001:400:f00::1/64).  *An IPv6 address is supported for the MGT interface on all M-Series appliances and Panorama virtual appliances deployed in a private cloud environment (ESXi, vCloud Air, KVM, or Hyper-V). An IPv6 address is not supported for the MGT interface on a Panorama virtual appliance deployed in a public cloud environment (Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, or Google Cloud Platform).*
Default IPv6 Gateway	If you assigned an IPv6 address to the interface, you must also assign an IPv6 address to the default gateway (the gateway must be on the same subnet as the interface).  *An IPv6 address is supported for the MGT interface on all M-Series appliances and Panorama virtual appliances deployed in a private cloud environment (ESXi, vCloud Air, KVM, or Hyper-V). An IPv6 address is not supported for the MGT interface on a Panorama virtual appliance deployed in a public cloud environment (Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, or Google Cloud Platform).*
Speed	Set the speed for the interface to 10Mbps, 100Mbps, 1Gbps, or 10Gbps (Eth4 and Eth5 only) at full or half duplex. Use the default auto-negotiate setting to have Panorama determine the interface speed.  *This setting must match the interface settings on neighboring network equipment. To ensure matching settings, select auto-negotiate if the neighboring equipment supports that option.*
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576 to 1,500; default is 1,500).
Device Management and Device Log Collection	Enable the interface (enabled by default on the MGT interface) for managing firewalls and Log Collectors and collecting their logs. You can enable multiple interfaces to perform these functions.
Collector Group Communication	Enable the interface for Collector Group communication (the default is the MGT interface). Only one interface can perform this function.
Syslog Forwarding	Enable the interface for forwarding syslogs (the default is the MGT interface). Only one interface can perform this function.

Interface Settings	Description
Device Deployment	Enable the interface for deploying software and content updates to firewalls and Log Collectors (the default is the MGT interface). Only one interface can perform this function.
Administrative Management Services	• **HTTP**—Enables access the Panorama web interface. HTTP uses plaintext, which is not as secure as HTTPS.  *Enable HTTPS instead of HTTP for management traffic on the interface.* • **Telnet**—Enables access the Panorama CLI. Telnet uses plaintext, which is not as secure as SSH. • **HTTPS**—Enables secure access to the Panorama web interface.  *Enable SSH instead of Telnet for management traffic on the interface.* • **SSH**—Enables secure access to the Panorama CLI.
Network Connectivity Services	The **Ping** service is available on any interface. You can use ping to test connectivity between the Panorama interface and external services. In a high availability (HA) deployment, HA peers use ping to exchange heartbeat backup information. The following services are available only on the MGT interface: • **SNMP**—Enables Panorama to process statistics queries from an SNMP manager. For details, see Enable SNMP Monitoring. • **User-ID**—Enables Panorama to redistribute user mapping information received from User-ID agents.
Permitted IP Addresses	Enter the IP addresses from which administrators can access Panorama on this interface. An empty list (default) specifies that access is available from any IP address.  *Do not leave this list blank; specify the IP addresses of Panorama administrators (only) to prevent unauthorized access.*

Panorama > High Availability

To enable high availability (HA) on Panorama, configure the settings as described in the following table.

Panorama HA Settings	Description
Setup Click Edit ( ) to configure the following settings.	
Enable HA	Select to enable HA.
Peer HA IP Address	Enter the IP address of the MGT interface on the peer.
Enable Encryption	When enabled, the MGT interface encrypts communication between the HA peers. Before enabling encryption, export the HA key from each HA peer and import the key into the other peer. You import and export the HA key on the **Panorama** > **Certificate Management** > **Certificates** page (see Manage Firewall and Panorama Certificates).  *HA connectivity uses TCP port 28 with encryption enabled and TCP port 28769 when encryption is not enabled.*
Monitor Hold Time (ms)	Enter the number of milliseconds that the system will wait before acting on a control link failure (range is 1,000 to 60,000; default is 3,000).
Election Settings Click Edit ( ) to configure the following settings.	
Priority (Required on the Panorama virtual appliance)	This setting determines which peer is the primary recipient for firewall logs. Assign one peer as **Primary** and the other as **Secondary** in the HA pair. When you configure Log Storage Partitions for a Panorama Virtual Appliance in Legacy Mode, you can use its internal disk (default) or a Network File System (NFS) for log storage. If you configure an NFS, only the primary recipient receives the firewall logs. If you configure internal disk storage, the firewalls send logs to both the primary and the secondary peer by default but you can change this by enabling **Only Active Primary Logs to Local Disk** in the Logging and Reporting Settings.
Preemptive	Select to enable the primary Panorama to resume active operation after recovering from a failure. When disabled, the secondary Panorama remains active even after the primary Panorama recovers from a failure.
HA Timer Settings	Your selection determines the values for the remaining HA election settings, which control the failover speed: • **Recommended**—Select for typical (default) failover timer settings. To see the associated values, select **Advanced** and **Load Recommended**. • **Aggressive**—Select for faster failover timer settings. To see the associated values, select **Advanced** and **Load Aggressive**.

Panorama HA Settings	Description
	• **Advanced**—Select to display the remaining HA election settings and customize their values. See the **Recommended** and **Aggressive** values for the following settings.
Promotion Hold Time (ms)	Enter the number of milliseconds (range is 0 to 60,000) the secondary Panorama peer waits before taking over after the primary peer goes down. The recommended (default) value is 2,000; the aggressive value is 500.
Hello Interval (ms)	Enter the number of milliseconds (range is 8,000 to 60,000) between hello packets that are sent to verify that the other peer is operational. The recommended (default) and aggressive value is 8,000.
Heartbeat Interval (ms)	Specify the frequency in milliseconds (range is 1,000 to 60,000) at which Panorama sends ICMP pings to the HA peer. The recommended (default) value is 2,000; the aggressive value is 1,000.
Preemption Hold Time (min)	This field applies only if you also select **Preemptive**. Enter the number of minutes (range is 1 to 60) the passive Panorama peer will wait before falling back to active status after it recovers from an event that caused failover. The recommended (default) and aggressive value is 1.
Monitor Fail Hold Up Time (ms)	Specify the number of milliseconds (range is 0 to 60,000) Panorama waits after a path monitor failure before attempting to re-enter the passive state. During this period, the passive peer is not available to take over for the active peer in the event of failure. This interval enables Panorama to avoid a failover due to the occasional flapping of neighboring devices. The recommended (default) and aggressive value is 0.
Additional Master Hold Up Time (ms)	Specify the number of milliseconds (range is 0 to 60,000) during which the preempting peer remains in the passive state before taking over as the active peer. The recommended (default) value is 7,000; the aggressive value is 5,000.
Path Monitoring Click Edit ( ) to configure HA path monitoring.	
Enabled	Select to enable path monitoring. Path monitoring enables Panorama to monitor specified destination IP addresses by sending ICMP ping messages to verify that they are responsive.
Failure Condition	Select whether a failover occurs when **Any** or **All** of the monitored path groups fail to respond.
Path Group To create a path group for HA path monitoring, click **Add** and complete the following fields.	
Name	Specify a name for the path group.
Enabled	Select to enable the path group.

Panorama HA Settings	Description
Failure Condition	Select whether a failure occurs when **Any** or **All** of the specified destination addresses fails to respond.
Ping Interval	Specify the number of milliseconds between the ICMP echo messages that verify that the path to the destination IP address is up (range is 1,000 to 60,000; default is 5,000).
Ping Count	Specify the number of failed pings before declaring a failure (range is 3 to 10; default is 3).
Destination IPs	Enter one or more destination IP addresses to monitor. Use commas to separate multiple addresses.

Panorama > Managed WildFire Clusters

- Panorama > Managed WildFire Clusters
- Panorama > Managed WildFire Appliances

You can manage WildFire appliances in clusters or as standalone appliances from a Panorama M-Series or virtual appliance. Managing clusters (**Panorama** > **Managed WildFire Clusters**) and managing standalone appliances (**Panorama** > **Managed WildFire Appliances**) share many common administrative and configuration tasks so both are included in the following topics.

After you add WildFire appliances to Panorama, use the web interface to add those appliances to and manage them as clusters or to manage them as standalone appliances.

- Managed WildFire Cluster Tasks
- Managed WildFire Appliance Tasks
- Managed WildFire Information
- Managed WildFire Cluster and Appliance Administration

Managed WildFire Cluster Tasks

You can create and remove WildFire appliance clusters from Panorama. Additionally, you can save configuration time when you import configurations from one cluster to another.

Task	Description
Create Cluster	As needed, **Create Cluster**, enter a name for the new cluster, and then click **OK**. Existing clusters that you configured locally and added to Panorama by adding the individual WildFire appliance nodes are listed along with their WildFire nodes and node roles (**Panorama** > **Managed WildFire Appliances**). The cluster name must be a valid subdomain name that begins with a lowercase character or number and that can contain hyphens only when they are not the first or last character in the cluster name—no spaces or other characters are allowed. The maximum length of a cluster name is 63 characters. After you create a cluster, you can add managed WildFire appliances to the cluster and manage them on Panorama. When you add a WildFire appliance to Panorama, you automatically register the appliance with Panorama. You can create a maximum of 10 managed WildFire clusters on Panorama and each cluster can have up to 20 WildFire appliance nodes. Panorama can manage up to an aggregate total of 200 standalone appliances and cluster nodes.
Import Cluster Config	**Import Cluster Config** to import an existing cluster configuration. If you select a cluster before you **Import Cluster Config**, the **Controller** and **Cluster** are automatically populated with the appropriate information for the selected cluster. If you do not select a cluster before you **Import Cluster Config**, then you must select the **Controller** and the **Cluster** populates automatically based on the Controller node you select.

Task	Description
	After you import the configuration, **Commit to Panorama** to save the imported candidate configuration in the Panorama running configuration.
Remove From Panorama	If you no longer need to manage a WildFire cluster from Panorama, **Remove From Panorama** and select **Yes** to confirm your action. After you remove a cluster from Panorama management, you can manage the cluster locally from a Controller node. You can add the cluster back in to the Panorama appliance at any time if you want to again manage the cluster centrally instead of locally.
Encrypt WildFire Cluster Appliance-to-Appliance Communications	To encrypt data communication between WildFire appliances in a cluster, **Enable** encryption under **Secure Cluster Communication**. WildFire uses either a predefined certificate or a custom certificate to communicate between appliances. Custom certificates are only used when you **Customize Secure Server Communication** and enable **Custom Certificate Only**. Encryption is required for WildFire clusters to operate in FIPS-CC mode. Custom certificates used in FIPS-CC mode must meet FIPS-CC requirements. After you enable secure cluster communication, you can add additional managed WildFire appliances to the cluster. Newly added appliances automatically use the secure cluster communication settings.

Managed WildFire Appliance Tasks

You can add, remove, and manage standalone WildFire appliances on a Panorama device. After you add standalone appliances, you can add them to WildFire appliance clusters as cluster nodes or you can manage them as individual standalone appliances.

Task	Description

Add Appliance	**Add Appliance** to add one or more WildFire appliances to a Panorama appliance for centralized management. Enter the serial number of each WildFire appliance on a separate row (new line). Panorama can manage up to an aggregate total of 200 WildFire cluster nodes and standalone WildFire appliances.
	On each WildFire appliance you want to manage on Panorama, configure the IP address or FQDN of the Panorama appliance (Panorama server) and, optionally, the backup Panorama server using the following WildFire appliance CLI commands:
	`set deviceconfig system panorama-server <ip-address | FQDN>`
	`set deviceconfig system panorama-server-2 <ip-address | FQDN>`

Import Config	Select a WildFire appliance and **Import Config** to import (only) the running configuration for that appliance to Panorama.

Task	Description
	After you import the configuration, **Commit to Panorama** to save the imported candidate configuration in the Panorama running configuration.
Remove	If you no longer need to manage a WildFire appliance from Panorama, **Remove** the appliance and select **Yes** to confirm your action. After you remove an appliance from Panorama management, you can manage the appliance locally using its CLI. If needed, you can add the appliance back into the Panorama appliance at any time if you want to again manage the appliance centrally instead of locally.

Managed WildFire Information

Select **Panorama** > **Managed WildFire Clusters** to display the following information for each managed cluster (you can also select standalone appliances from this page and display their information) or select **Panorama** > **Managed WildFire Appliances** to display the information for standalone appliances.

Unless noted, the information in the following table applies to both WildFire clusters and standalone appliances. The information previously configured for a cluster or appliance is pre-populated.

Managed WildFire Information	Description
Appliance	The name of the appliance. The Managed WildFire Clusters view displays appliances grouped by cluster, includes the standalone appliances available to add to a cluster, and includes the serial number (in parentheses) with the appliance name (the serial number is not part of the name).
Serial Number (Managed WildFire Appliances view only)	The serial number of the appliance. The Managed WildFire Clusters view displays the serial number in the same column as the appliance name (the serial number is not part of the name).
Software Version	The software version installed and running on the appliance.
IP Address	The IP address of the appliance.
Connected	The connection state between the appliance and Panorama—either Connected or Disconnected.
Cluster Name	The name of the cluster in which the appliance is included as a node; nothing displays here for a standalone appliance.
Analysis Environment	The analysis environment (vm1, vm2, vm3, vm4, or vm5). Each analysis environment represents a set of operating systems and applications: • vm-1 supports Windows XP, Adobe Reader 9.3.3, Flash 9, PE, PDF, and Office 2003 and earlier Office releases. • vm-2 supports Windows XP, Adobe Reader 9.4.0, Flash 10n, PE, PDF, and Office 2007 and earlier Office releases.

Managed WildFire Information	Description
	• vm-3 supports Windows XP, Adobe Reader 11, Flash 11, PE, PDF, and Office 2010 and earlier Office releases. • vm-4 supports Windows 7 32-bit, Adobe Reader 11, Flash 11, PE, PDF, and Office 2010 and earlier Office releases. • vm-5 supports Windows 7 64-bit, Adobe Reader 11, Flash 11, PE, PDF, and Office 2010 and earlier Office releases.
Content	The version number of the content release version.
Role	The appliance role: • **Standalone**—The appliance is not a cluster node. • **Controller**—The appliance is the cluster Controller node. • **Controller Backup**—The appliance is the cluster Controller backup node. • **Worker**—The appliance is a Worker node in the cluster.
Config Status	The configuration synchronization status of the appliance. The Panorama appliance checks for WildFire appliance settings and reports configuration differences between the appliance configuration and the configuration saved for that appliance on Panorama. • **In Sync**—The appliance configuration is in sync with its saved configuration on Panorama. • **Out of Sync**—The appliance configuration is not in sync with its saved configuration on Panorama. You can mouse over the eyeglass to display the cause of the sync failure.
Cluster Status (Managed WildFire Clusters page only)	Cluster Status displays three types of information for each cluster node: • Services available (normal operating conditions): • **wfpc** (WildFire Private Cloud)—The malware sample analysis and reporting service. • **signature**—The local signature generation service. • Progress of operations—the operation name followed by a colon (:) and the status: • **Operations**—Status for decommission, suspend, and reboot operations. • **Progress status**—Operation status notifications are the same for each operation: requested, ongoing, denied, success, or fail. For example, if you suspend a node and the operation is ongoing, Cluster Status displays `suspend:ongoing`, or if you reboot a node and the operation has been requested but has not yet begun, Cluster Status displays `reboot:requested`. • Error conditions: Cluster Status displays the following error conditions: • **Cluster**—`cluster:offline` or `cluster:splitbrain`. • **Service**—`service:suspended` or `service:none`.

Managed WildFire Information	Description
Last Commit State	`Commit succeeded` if the most recent commit succeeded or `commit failed` if the most recent commit failed. View details about the last commit by selecting the state.
Utilization > View	
View	**View** cluster or appliance utilization statistics. You can view only individual appliances (**Panorama** > **Managed WildFire Appliances**) or you can view only cluster statistics (**Panorama** > **Managed WildFire Clusters**). • **Appliance**—(Standalone appliance view only) The appliance serial number. • **Cluster**—(Cluster view only) The cluster name. You can also select a different cluster to view. • **Duration**—Displays the time period for which statistics are collected and displayed. You can select different durations: • **15 Min** • **Last Hour** • **Last 24 Hours (default)** • **Last 7 Days** • **All** The **Utilization View** has four tabs and, on each tab, you determine what is displayed based on your configured **Duration**.
General Tab	The **General** tab displays aggregated resource utilization statistics for a cluster or an appliance. The other tabs display more granular information about resource utilization by file type: • **Total Disk Usage**—The total cluster or appliance disk usage. • **Verdict**—The **Total** number of verdicts, the number of each verdict type assigned to files—**Malware**, **Grayware**, and **Benign**; and how many verdicts were **Error** verdicts. • **Sample Statistics**—The total number of samples **Submitted** and **Analyzed** and how many samples are **Pending** analysis. • **Analysis Environment & System Utilization**: • **File Type Analyzed**—The type of file that was analyzed—**Executable**, **Non-Executable**, or **Links**. • **Virtual Machine Usage**—The number of virtual machines used for each file type analyzed and how many virtual machines are available to analyze each file type. For example, for Executable files, VM usage could be 6/10 (six VMs used and ten VMs available). • **Files Analyzed**—The number of files of each type that were analyzed.
Executable, Non-Executable, and Links Tabs	The **Executable**, **Non-Executable**, and **Links** display similar information about each type of file: • **Verdict**—Details about verdicts by file type. You can filter the results: • **Search box**—Enter search terms to filter the verdicts. The search box indicates the number of file types (items) in the list. After you enter

Managed WildFire Information	Description
	search terms, apply the filter (→) or clear the filter (×) and enter a different set of terms. • **File Type**—List files by type. For example, the **Executable** tab displays .exe and .dll file types; the **Non-Executable** tab displays .pdf, .jar, .doc, .ppt, .xls, .docx, .pptx, .xlsx, .rtf, class, and .swf file types; and the **Links** tab displays elink file type information. • For each **File Type**, the total number of verdicts for **Malware**, **Grayware**, and **Benign** files, the number of **Error** verdicts, and the **Total** number of verdicts are displayed on each tab. • **Sample Statistics**—Details about sample analysis by file type. • **Search box**—Same as the **Verdict** search box. • **File Type**—Same as the **Verdict File Type**. • For each **File Type**, the total number of files **Submitted** for analysis, the total number **Analyzed**, and the number **Pending** analysis are displayed on each tab.
Firewalls Connected > View	
View	**View** information about the firewalls connected to the cluster or the appliance. You can view only individual appliances (**Panorama** > **Managed WildFire Appliances**) or you can view only cluster statistics (**Panorama** > **Managed WildFire Clusters**). • **Appliance**—(Standalone appliance view only) The appliance serial number. • **Cluster**—(Cluster view only) The cluster name, you can also select a different cluster to view. • **Refresh**—Refresh the display.
Registered and Submitting Samples Tabs	The **Registered** tab displays information about firewalls registered to the cluster or appliance, regardless of whether the firewalls are submitting samples. The **Submitting Samples** tab displays information about firewalls that are actively submitting samples to the WildFire cluster or appliance. The type of information displayed on these tabs and how to filter the information is similar for both: • **Search box**—Enter search terms to filter the list of firewalls. The search box indicates the number of firewalls (items) in the list. After you enter search terms, apply the filter (→) or clear the filter (×) and enter a different set of terms. • **S/N**—The serial number of the firewall. • **IP Address**—The IP address of the firewall. • **Model**—The model number of the firewall. • **Software Version**—The software version installed and running on the firewall.

Managed WildFire Cluster and Appliance Administration

Select **Panorama** > **Managed WildFire Clusters** and select a cluster to manage or select a WildFire appliance (**Panorama** > **Managed WildFire Appliances**) to manage a standalone appliance. The **Panorama** > **Managed WildFire Cluster** view lists cluster nodes (WildFire appliances that are members of the cluster) and standalone appliances so that you can add available appliances to a cluster. Because the cluster manages the nodes, selecting a cluster node provides only limited management capability.

Unless noted, the settings and descriptions in the following table apply to both WildFire clusters and WildFire standalone appliances. Information previously configured on a cluster or appliance is prepopulated. You must first commit changes and additions to the information on Panorama and then push the new configuration to the appliances.

Setting	Description
General tab	
Name	The cluster or appliance **Name** or the appliance serial number.
Enable DNS (WildFire clusters only)	**Enable DNS** service for the cluster.
Register Firewall To	The domain name to which you register firewalls. Format must be **`wfpc.service.<`***cluster-name***`>.<`***domain***`>`**. For example, the default domain name is **`wfpc.service.mycluster.paloaltonetworks.com`**.
Content Update Server	Enter the **Content Update Server** location or use the default **`wildfire.paloaltonetworks.com`** so that the cluster or appliance receives content updates from the closest server in the Content Delivery Network infrastructure. Connecting to the global cloud gives you the benefit of accessing signatures and updates based on threat analysis from all sources connected to the cloud, instead of relying only on the analysis of local threats.
Check Server Identity	**Check Server Identity** to confirm the identity of the update server by matching the common name (CN) in the certificate with the IP address or FQDN of the server.
WildFire Cloud Server	Enter the global **WildFire Cloud Server** location or use the default **`wildfire.paloaltonetworks.com`** so that the cluster or appliance can send information to the closest server. You can choose whether to send information and what types of information to send to the global cloud (**WildFire Cloud Services**).
Sample Analysis Image	Select the VM image for the cluster or appliance to use for sample analysis (default is vm-5). You can Get a Malware Test File (WildFire API) to see the result of the sample analysis.
WildFire Cloud Services	If the cluster or appliance is connected to the global WildFire Cloud Server, you can choose whether to **Send Analysis Data**, **Send Malicious Samples**, **Send Diagnostics** to the global cloud or any combination of the three. You can also choose whether to perform a **Verdict Lookup** in the global cloud. Sending information to the global cloud benefits the entire community of WildFire

Setting	Description
	users because the shared information increases the ability of every appliance to identify malicious traffic and prevent it from traversing the network.
Sample Data Retention	The number of days to retain benign or grayware samples and malicious samples: • **Benign/Grayware** samples—Range is 1 to 90; default is 14. • **Malicious** samples—Minimum is 1 and there is no maximum (indefinite); default is indefinite.
Analysis Environment Services	**Environment Networking** enables virtual machines to communicate with the internet. You can select **Anonymous Networking** to make network communication anonymous but you must select **Environment Networking** before you can enable **Anonymous Networking**. Different network environments produce different types of analysis loads depending on whether more documents need to be analyzed or more executable files need to be analyzed. You can configure your Preferred Analysis Environment to allocate more resources to **Executables** or to **Documents**, depending on the needs of your environment. The **Default** allocation is balanced between **Executables** and **Documents**. The amount of available resources depends on how many WildFire nodes are in the cluster.
Signature Generation	Select whether you want the cluster or appliance to generate signatures for AV, DNS, URLs, or any combination of the three.
Appliance tab	
Hostname (Standalone WildFire appliance only)	Enter the hostname of the WildFire appliance.
Panorama Server	Enter the IP address or FQDN of the appliance or of the primary Panorama managing the cluster.
Panorama Server 2	Enter the IP address or FQDN of the appliance or of the backup Panorama managing the cluster.
Domain	Enter the domain name of the appliance cluster or appliance.
Primary DNS Server	Enter the IP address of the primary DNS Server.
Secondary DNS Server	Enter the IP address of the secondary DNS Server.
Timezone	Select the time zone to use for the cluster or appliance.
Latitude (Standalone WildFire appliance only)	Enter the latitude of the WildFire appliance.

Setting	Description
Longitude (Standalone WildFire appliance only)	Enter the longitude of the WildFire appliance.
Primary NTP Server	Enter the IP address of the primary NTP Server and set the Authentication Type to **None** (default), **Symmetric Key**, or **Autokey**. Setting the Authentication Type to **Symmetric Key** reveals four more fields: • **Key ID**—Enter the authentication key ID. • **Algorithm**—Set the authentication algorithm to **SHA1** or **MD5**. • **Authentication Key**—Enter the authentication key. • **Confirm Authentication Key**—Enter the authentication key again to confirm it.
Secondary NTP Server	Enter the IP address of the secondary NTP Server and set the Authentication Type to **None** (default), **Symmetric Key**, or **Autokey**. Setting the Authentication Type to **Symmetric Key** reveals four more fields: • **Key ID**—Enter the authentication key ID. • **Algorithm**—Set the authentication algorithm to **SHA1** or **MD5**. • **Authentication Key**—Enter the authentication key. • **Confirm Authentication Key**—Enter the authentication key again to confirm it.
Login Banner	Enter a banner message that displays when users log in to the cluster or appliance.
Logging tab (Includes System tab and Configuration tab)	
Add	**Add** log forwarding profiles (**Panorama** > **Managed WildFire Clusters** > <*cluster*> > **Logging** > **System** or **Panorama** > **Managed WildFire Clusters** > <*cluster*> > **Logging** > **Configuration**) to forward: • system or configuration logs as SNMP traps to SNMP trap receivers. • syslog messages to syslog servers. • email notifications to email servers. • HTTP requests to HTTP servers. No other log types are supported (see Device > Log Settings). The Log Forwarding profiles specify which logs to forward and to which destination servers. For each profile, complete the following: • **Name**—A name that identifies the log settings (up to 31 characters) that consists of alphanumeric characters and underscores only—spaces and special characters are not allowed. • **Filter**—By default, the Panorama appliance forwards **All Logs** of the specified profile. To forward a subset of the logs, select a filter (**severity eq critical**, **severity eq high**, **severity eq informational**, **severity eq low**, or **severity eq medium**) or select **Filter Builder** to create a new filter. • **Description**—Enter a description (up to 1,023 characters) to explain the purpose of the profile.

Setting	Description
Add > Filter > Filter Builder	Use **Filter Builder** to create new log filters. Select **Create Filter** to construct filters and, for each query in a new filter, specify the following settings and then **Add** the query: • **Connector**—Select the connector logic (**and** or **or**). Select **Negate** if you want to apply negation. For example, to avoid forwarding a subset of log descriptions, select **Description** as the Attribute, select **contains** as the Operator, and enter the description string as the Value to identify the description or descriptions that you don't want to forward. • **Attribute**—Select a log attribute. The options vary by log type. • **Operator**—Select the criterion that determines how the attribute applies (such as **contains**). The options vary by log type. • **Value**—Specify the attribute value to match. • **Add**—Add the new filter. To display or export logs that the filter matches, select **View Filtered Logs**. • To find matching log entries, you can add artifacts to the search field, such as an IP address or a time range. • Select the time period for which you want to see logs: **Last 15 Minutes**, **Last Hour**, **Last 6 Hrs**, **Last 12 Hrs**, **Last 24 Hrs**, **Last 7 Days**, **Last 30 Days**, or **All** (default). • Use the options to the right of the time period drop-down to apply, clear, add, save, and load filters: • **Apply filters** ( )—Display log entries that match the terms in the search field. • **Clear filters** ( )—Clear the filter field. • **Add a new filter** ( )—Define new search criteria (takes you to Add Log Filter, which is similar to create filters). • **Save a filter** ( )—Enter a name for the filter and then click **OK**. • **Use a saved filter** ( )—Add a saved filter to the filter field. • **Export to CSV** ( )—Export logs to a CSV-formatted report and then **Download file**. By default, the report contains up to 2,000 lines of logs. To change the line limit for generated CSV reports, select **Device** > **Setup** > **Management** > **Logging and Reporting Settings** > **Log Export and Reporting** and enter a new **Max Rows in CSV Export** value. You can change the number and order of entries displayed per page and you can use the paging controls at the bottom left of the page to navigate through the log list. Log entries are retrieved in blocks of 10 pages. • **per page**—Use the drop-down to change the number of log entries per page (**20**, **30**, **40**, **50**, **75**, or **100**). • **ASC** or **DESC**—Select **ASC** to sort results in ascending order (oldest log entry first) or **DESC** to sort in descending order (newest log entry first). The default is **DESC**. • **Resolve Hostname**—Select to resolve external IP addresses to domain names. • **Highlight Policy Actions**—Specify an action and select to highlight log entries that match the action. The filtered logs are highlighted in the following colors:

Setting	Description
	• Green—Allow • Yellow—Continue or override • Red—Deny, drop, drop-icmp, rst-client, reset-server, reset-both, block-continue, block-override, block-url, drop-all, sinkhole
Delete	Select and then **Delete** the log forwarding settings you want to remove from the System or Configuration log list.
Authentication tab	
Authentication Profile	Select a configured authentication profile to define the authentication service that validates the login credentials of the WildFire appliance or Panorama administrators.
Failed Attempts	Enter the number of failed login attempts that the WildFire appliance allows on the CLI before locking out the administrator (range is 0 to 10; default is 10). Limiting login attempts helps protect the WildFire appliance from brute force attacks. A value of 0 specifies unlimited login attempts.  *If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, then the administrator is indefinitely locked out until another administrator manually unlocks the locked-out administrator. If no other administrator has been created, you must reconfigure the Failed Attempts and Lockout Time settings on Panorama and push the configuration change to the WildFire appliance. To ensure that an administrator is never locked out, use the default (**0**) value for both Failed Attempts and Lockout Time.*  *Set the number of Failed Attempts to 5 or fewer to accommodate a reasonable number of retries in case of typing errors, while preventing malicious systems from trying brute force methods to log in to the WildFire appliance.*
Lockout Time (min)	Enter the number of minutes for which the WildFire appliance locks out an administrator from access to the CLI after reaching the **Failed Attempts** limit (range is 0 to 60; default is 5). A value of 0 means the lockout applies until another administrator manually unlocks the account.  *If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, then the administrator is indefinitely locked out until another administrator manually unlocks the locked-out administrator. If no other administrator has been created, you must reconfigure the Failed Attempts and Lockout Time settings on Panorama and push the configuration change to the WildFire appliance. To ensure that an administrator is never locked out, use the default (**0**) value for both Failed Attempts and Lockout Time.*

Setting	Description
	 *Set the Lockout Time to at least 30 minutes to prevent continuous login attempts from a malicious actor.*
Idle Timeout (min)	Enter the maximum number of minutes without any activity on the CLI before an administrator is automatically logged out (range is 0 to 1,440; default is None). A value of 0 means that inactivity does not trigger an automatic logout.  *Set the Idle Timeout to 10 minutes to prevent unauthorized users from accessing the WildFire appliance if an administrator leaves a session open.*
Max Session Count	Enter the number of active sessions the administrator can have open concurrently, The default is 0, which means that the WildFire appliance can have an unlimited number of concurrently active sessions.
Max Session time	Enter the number of minutes the administrator can be logged in before being automatically logged out. The default is 0, which means that the administrator can be logged in indefinitely even if idle.
Local Administrators	Add and configure new administrators for the WildFire appliance. These administrators are unique to the WildFire appliance are managed from this page (**Panorama** > **Managed WildFire Appliances** > **Authentication**).
Panorama Administrators	Import existing administrators configured on Panorama. These administrators are created on Panorama and imported into the WildFire appliance.
Clustering tab (Managed WildFire Clusters only) and Interfaces tab (Managed WildFire Appliances only) You must add appliances to Panorama to manage interfaces and add appliances to clusters to manage node interfaces.	
Appliance (Clustering tab only)	Select a cluster node to access the Appliance and Interfaces tabs for that node. The Appliance tab node information is prepopulated and not configurable except for the hostname. The Interfaces tab lists the node interfaces. Select an interface to manage it as described in: • Interface Name Management • Interface Name Analysis Environment Network • Interface Name Ethernet2 • Interface Name Ethernet3
Interface Name Management	The management interface is Ethernet0. Configure or view management interface settings: • **Speed and Duplex**—Select **auto-negotiate** (default), **10Mbps-half-duplex**, **10Mbps-full-duplex**, **100Mbps-half-duplex**, **100Mbps-full-duplex**, **1Gbps-half-duplex**, or **1Gbps-full-duplex**. • **IP Address**—Enter the interface IP address. • **Netmask**—Enter the interface netmask. • **Default Gateway**—Enter the IP address of the default gateway. • **MTU**—Enter the MTU in bytes (range is 576 to 1,500; default is 1,500).

Setting	Description
	• **Management Services**—Enable the management services you want to support. You can support **Ping**, **SSH**, and **SNMP** services. Configure proxy settings if you use a proxy server to connect to the Internet: • **Server**—IP address of the proxy server. • **Port**—Port number configured on the proxy server to listen for Panorama device requests. • **User**—Username configured on the proxy server for authentication. • **Password** and **Confirm Password**—Password configured on the proxy server for authentication. • **Clustering Services** (Clustering tab only)—Select the HA service: • **HA**—If there are two Controller nodes in the cluster, you can configure the management interface as an HA interface so that management information is available to both Controller nodes. If the cluster node you are configuring is the primary Controller node, mark it as the **HA** interface. Depending on how you use the WildFire appliance Ethernet interfaces, you can, alternatively, configure Etherent2 or Ethernet3 as the HA and HA Backup interfaces on the primary and backup Controller nodes respectively. For example, you can use Ethernet 2 as the HA and HA Backup interface. The HA and HA Backup interfaces must be the same interface (management, Ethernet2, or Ethernet3) on the primary and backup Controller nodes. You cannot use Ethernet1 as the HA/HA Backup interface. • **HA Backup**—If the cluster node you are configuring is the backup Controller node, mark it as the **HA Backup** interface. Specify IP addresses that are permitted on the interface: • **Search box**—Enter search terms to filter the permitted IP address list. The search box indicates the number of IP addresses (items) in the list so you know how long the list is. After you enter search terms, apply the filter (→) or clear the filter (×) and enter a different set of terms. • **Add**—**Add** a permitted IP address. • **Delete**—Select and **Delete** the IP address or addresses you want to remove from management interface access.
Interface Name Analysis Environment Network	Configure settings for the WildFire appliance cluster or standalone WildFire appliance analysis environment network interface (Ethernet1, also known as the VM interface): • **Speed and Duplex**—Set to **auto-negotiate** (default), **10Mbps-half-duplex**, **10Mbps-full-duplex**, **100Mbps-half-duplex**, **100Mbps-full-duplex**, **1Gbps-half-duplex**, or **1Gbps-full-duplex**. • **IP Address**—Enter the interface IP address. • **Netmask**—Enter the interface netmask. • **Default Gateway**—Enter the IP address of the default gateway. • **MTU**—Enter the MTU in bytes (range is 576 to 1,500; default is 1,500). • **DNS Server**—Enter the DNS server IP address. • **Link State**—Set the interface link state to **Up** or **Down**.

Setting	Description
	• Management Services—Enable **Ping** if you want the interface to support ping services. Specify IP addresses that are permitted on the interface: • **Search box**—Enter search terms to filter the permitted IP address list. The search box indicates the number of IP addresses (items) in the list so you know how long the list is. After you enter search terms, apply the filter (→) or clear the filter (×) and enter a different set of terms. • **Add**—**Add** a permitted IP address. • **Delete**—Select the IP address or IP addresses you want to remove from management interface access and then **Delete**.
Interface Name Ethernet2 Interface Name Ethernet3	You can set the same parameters for the Ethernet2 and Ethernet3 interfaces: • **Speed and Duplex**—Set to **auto-negotiate** (default), **10Mbps-half-duplex**, **10Mbps-full-duplex**, **100Mbps-half-duplex**, **100Mbps-full-duplex**, **1Gbps-half-duplex**, or **1Gbps-full-duplex**. • **IP Address**—Enter the interface IP address. • **Netmask**—Enter the interface netmask. • **Default Gateway**—Enter the IP address of the default gateway. • **MTU**—Enter the MTU in bytes (range is 576 to 1,500; default is 1,500). • Management Services—Enable **Ping** if you want the interface to support ping services. • **Clustering Services**—Select cluster services: • **HA**—If there are two Controller nodes in the cluster, you can configure the Ethernet2 or the Ethernet3 interface as an HA interface so that management information is available to both Controller nodes. If the cluster node you are configuring is the primary Controller node, mark it as the **HA** interface. Depending on how you use the WildFire appliance Ethernet interfaces, alternatively, you can configure the management interface (Ethernet1) as the HA and HA Backup interfaces on the primary and backup Controller nodes, respectively. The HA and HA Backup interfaces must be the same interface (management, Ethernet2, or Ethernet3) on the primary and backup Controller nodes. You cannot use Ethernet1 as the HA/HA Backup interface. • **HA Backup**—If the cluster node you are configuring is the backup Controller node, mark it as the **HA Backup** interface. • **Cluster Management**—Configure the Ethernet2 or Ethernet3 interface as the interface used for cluster-wide management and communication.
Role (Clustering tab only)	When a cluster has member appliances, the appliance roles can be Controller, Controller Backup, or Worker. Select **Controller** or **Backup Controller** to change the WildFire appliance used for each role from the appliances in the cluster. Changing the Controller results in data loss during the role change.
Browse (Clustering tab only)	The **Clustering** tab lists the WildFire appliance nodes in the cluster. **Browse** to view and add standalone WildFire appliances that the Panorama device already manages:

Setting	Description
	• **Search box**—Enter search terms to filter the node list. The search box indicates the number of appliances (items) in the list so you know how long the list is. After you enter search terms, apply the filter (→) or clear the filter (×) and enter a different set of terms. • **Add Nodes**—Add (⊕) nodes to the cluster. The first WildFire appliance you add to a cluster automatically becomes the Controller node. The second WildFire appliance you add automatically becomes the Controller Backup node. You can add up to 20 WildFire appliances to a cluster. After adding the Controller and Controller Backup nodes, all subsequent added nodes are Worker nodes.
Delete (Clustering tab only)	Select one or more appliances from the Appliance list and then **Delete** them from the cluster. You can remove a Controller node only if there are two Controller nodes in the cluster.
Manage Controller (Clustering tab only)	Select **Manage Controller** to specify a **Controller** and a **Controller Backup** from the WildFire appliance nodes that belong to the cluster. The current Controller node and backup Controller node are selected by default. The backup Controller node can't be the same node as the primary Controller node.
Communication tab	
Customize Secure Server Communication	• **SSL/TLS Service Profile**—Select an SSL/TLS service profile from the drop-down. This profile defines the certificate and supported SSL/TLS versions that connected devices use to communicate with WildFire. • **Certificate Profile**—Select a certificate profile from the drop-down. This certificate profile defines certificate revocation checking behavior and the root CA used to authenticate the certificate chain presented by the client. • **Custom Certificate Only**—When enabled, WildFire only accepts custom certificates for authentication with connecting devices. • **Check Authorization List**—Client devices connecting to WildFire are checked against the authorization list. A device need match only one item on the list to be authorized. If no match is found, the device is not authorized. • **Authorization List**—**Add** an Authorization List and complete the following fields to set criteria for authorizing client devices. The Authorization List supports a maximum of 16 entries. • **Identifier**—Select **Subject** or **Subject Alt. Name** as the authorization identifier. • **Type**—If you selected **Subject Alt. Name** as the Identifier, then select **IP**, **hostname**, or **e-mail** as the type of the identifier. If you selected **Subject**, then common-name is the identifier type. • **Value**—Enter the identifier value.
Secure Client Communication	Using **Secure Client Communication** ensures that WildFire uses configured custom certificates (instead of the default predefined certificate) to authenticate SSL connections with another WildFire appliance.

Setting	Description
	• **Predefined**—(default) There is no device certificate configured—WildFire uses the default predefined certificate. • **Local**—WildFire uses a local device certificate and the corresponding private key generated on the firewall or imported from an existing enterprise PKI server. • **Certificate**: Select the local device certificate. • **Certificate Profile**: Select the Certificate Profile from the drop-down. • **SCEP**—WildFire uses a device certificate and private key generated by a Simple Certificate Enrollment Protocol (SCEP) server. • **SCEP Profile**: Select a SCEP Profile from the drop-down. • **Certificate Profile**: Select the Certificate Profile from the drop-down.
Secure Cluster Communication	Select **Enable** to encrypt communications between WildFire appliances. The default certificate uses the predefined certificate type. To use a user-defined custom certificate, you must configure **Customize Secure Server Communication** and enable **Custom Certificate Only**.

Panorama > Administrators

Select **Panorama** > **Administrators** to create and manage accounts for Panorama administrators.

If you log in to Panorama as an administrator with a superuser role, you can unlock the accounts of other administrators by clicking the lock icons in the Locked User column. A locked out administrator cannot access Panorama. Panorama locks out administrators who exceed the allowed number of failed successive attempts to access Panorama as defined in the **Authentication Profile** assigned to their accounts (see Device > Authentication Profile).

To create an administrator account, click **Add** and configure the settings as described in the following table.

Administrator Account Settings	Description
Name	Enter a login username for the administrator (up to 15 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, hyphens, and underscores.
Authentication Profile	Select an authentication profile or sequence to authenticate this administrator. For details, see Device > Authentication Profile or Device > Authentication Sequence.
Use only client certificate authentication (Web)	Select to use client certificate authentication for web interface access. If you select this option, a username (**Name**) and **Password** are not required.
Password/Confirm Password	Enter and confirm a case-sensitive password for the administrator (up to 15 characters). To ensure security, Palo Alto Networks recommends that administrators change their passwords periodically using a combination of lowercase letters, uppercase letters, and numbers. Be sure to use the best practices for password strength to ensure a strict password. Device Group and Template administrators cannot access **Panorama** > **Administrators**. To change their local password, these administrators click their username (beside **Logout** at the bottom of the web interface). This also applies to administrators with a custom Panorama role in which access to **Panorama** > **Administrators** is disabled. You can use password authentication in conjunction with an **Authentication Profile** (or sequence) or with local database authentication. You can set password expiration parameters by selecting a **Password Profile** (see Device > Password Profiles) and setting Minimum Password Complexity parameters (see Device > Setup > Management), but only for administrative accounts that Panorama authenticates locally.
Use Public Key Authentication (SSH)	Select to use SSH public key authentication: click **Import Key**, **Browse** to select the public key file, and click **OK**. The Administrator dialog displays the uploaded key in the read-only text area. Supported key file formats are IETF SECSH and OpenSSH. Supported key algorithms are DSA (1024 bits) and RSA (768 to 4096 bits).

Administrator Account Settings	Description
	If public key authentication fails, Panorama presents a login and password prompt.
Administrator Type	The type selection determines the administrative role options: • **Dynamic**—Roles that provide access to Panorama and managed firewalls. When new features are added, Panorama automatically updates the definitions of dynamic roles; you never need to manually update them. • **Custom Panorama Admin**—Configurable roles that have read-write access, read-only access, or no access to Panorama features. • **Device Group and Template Admin**—Configurable roles that have read-write access, read-only access, or no access to features for the device groups and templates that are assigned to the access domains you select for this administrator.
Admin Role (Dynamic administrator type)	Select a predefined role: • **Superuser**—Full read-write access to Panorama and all device groups, templates, and managed firewalls. • **Superuser (Read Only)**—Read-only access to Panorama and all device groups, templates, and managed firewalls. • **Panorama administrator**—Full access to Panorama except for the following actions: • Create, modify, or delete Panorama or firewall administrators and roles. • Export, validate, revert, save, load, or import a configuration (**Device** > **Setup** > **Operations**). • Configure a **Scheduled Config Export** in the **Panorama** tab.
Profile (Custom Panorama Admin administrator type)	Select a custom Panorama role (see Panorama > Managed Devices > Summary).
Access Domain to Administrator Role (Device Group and Template Admin administrator type)	For each access domain (up to 25) you want to assign to the administrator, **Add** an **Access Domain** from the drop-down (see Panorama > Access Domains) and then click the adjacent Admin Role cell and select a custom Device Group and Template administrator role from the drop-down (see Panorama > Managed Devices > Summary). When administrators with access to more than one domain log in to Panorama, an **Access Domain** drop-down appears in the footer of the web interface. Administrators can select any assigned **Access Domain** to filter the monitoring and configuration data that Panorama displays. The **Access Domain** selection also filters the firewalls that the **Context** drop-down displays. *If you use a RADIUS server to authenticate administrators, you must map administrator roles and access domainstoRADIUS VSAs. Because VSA strings support a limited number of characters, if you configure the maximum number of access domain/role*

Administrator Account Settings	Description
	pairs (25) for an administrator, the Name values for each access domain and each role must not exceed an average of 9 characters.
Password Profile	Select a **Password Profile** (see Device > Password Profiles).

Panorama > Admin Roles

Admin Role profiles are custom roles that define the access privileges and responsibilities of administrators. For example, the roles assigned to an administrator control which reports he or she can generate and which device group or template configurations the administrator can view or change.

For a Device Group and Template administrator, you can assign a separate role to each access domain that is assigned to the administrative account (see Panorama > Access Domains). Mapping roles to access domains enables you to achieve very granular control over the information that administrators can access on Panorama. For example, consider a scenario where you configure an access domain that includes all the device groups for firewalls in your data centers and you assign that access domain to an administrator who is allowed to monitor data center traffic but who is not allowed to configure the firewalls. In this case, you would map the access domain to a role that enables all monitoring privileges but disables access to device group settings.

To create an Admin Role profile, **Add** a profile and configure the settings as described in the following table.

If you use a RADIUS server to authenticate administrators, map the administrator roles and access domains to RADIUS Vendor Specific Attributes (VSAs).

Panorama Administrator Role Settings	Description
Name	Enter a name to identify this administrator role (up to 31 characters). The name is case-sensitive, must be unique and can contain only letters, numbers, spaces, hyphens, and underscores.
Description	(Optional) Enter a description of the role.
Role	Select the scope of administrative responsibility: **Panorama** or **Device Group and Template**.
Web UI	Select from the following options to set the type of access permitted for specific features in the Panorama context (**Web UI list**) and firewall context (**Context Switch UI list**): • **Enable** ( )—Read and write access • **Read Only** ( )—Read-only access • **Disable** ( )—No access
XML API (Panorama role only)	Select the type of XML API access (**Enable** or **Disable**) for Panorama and managed firewalls: • **Report**—Access to Panorama and firewall reports. • **Log**—Access to Panorama and firewall logs. • **Configuration**—Permissions to retrieve or modify Panorama and firewall configurations. • **Operational Requests**—Permissions to run operational commands on Panorama and firewalls. • **Commit**—Permissions to commit Panorama and firewall configurations. • **User-ID Agent**—Access to the User-ID agent.

Panorama Administrator Role Settings	Description
	• **Export**—Permissions to export files from Panorama and firewalls (such as configurations, block or response pages, certificates, and keys). • **Import**—Permissions to import files into Panorama and firewalls (such as software updates, content updates, licenses, configurations, certificates, block pages, and custom logs).
Command Line (Panorama role only)	Select the type of role for CLI access: • **None**—(Default) Access to the Panorama CLI not permitted. • **superuser**—Full access to **Panorama**. • **superreader**—Read-only access to **Panorama**. • **panorama-admin —**Full access to **Panorama** except for the following actions: • Create, modify, or delete Panorama administrators and roles. • Export, validate, revert, save, load, or import a configuration. • Schedule configuration exports.
REST API (Panorama role only)	Select the type of access (**Enable**, **Read Only**, or **Disable**) that applies to each REST API endpoint for Panorama and managed firewalls. You can assign role access to endpoints in the following categories. • Objects • Policies • Network • Device

Panorama > Access Domains

Access domains control the access that Device Group and Template administrators have to specific device groups (to manage policies and objects), to templates (to manage network and device settings), to the web interface of managed firewalls (through context switching), and to the REST API of managed firewalls. You can define up to 4,000 access domains and manage them locally or by using RADIUS Vendor-Specific Attributes (VSAs), TACACS+ VSAs, or SAML attributes. To create an access domain, **Add** a domain and configure the settings as described in the following table.

Access Domain Settings	Description
Name	Enter a name for the access domain (up to 31 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, hyphens, and underscores.
Shared Objects	Select one of the following access privileges for the objects that device groups in this access domain inherit from the Shared location. Regardless of privilege, administrators can't override shared or default (predefined) objects. • **read**—Administrators can display and clone shared objects but cannot perform any other operations on them. When adding non-shared objects or cloning shared objects, the destination must be a device group within the access domain, not Shared. • **write**—Administrators can perform all operations on shared objects. This is the default value. • **shared-only**—Administrators can add objects only to Shared. Administrators can also display, edit, and delete shared objects but cannot move or clone them. A consequence of this selection is that administrators cannot perform any operations on non-shared objects other than to display them.
Device Groups	Enable or disable read-write access for specific device groups in the access domain. You can also click **Enable All** or **Disable All**. Enabling read-write access for a device group automatically enables the same access for its descendants. If you manually disable a descendant, access for its highest ancestor automatically changes to read-only. By default, access is disabled for all device groups. If you want the list to display only specific device groups, select the device group names and **Filter Selected**. *If you set the access for shared objects to shared-only, Panorama applies read-only access to any device groups for which you specify read-write access.*
Templates	For each template or template stack you want to assign, click **Add** and select it from the drop-down.
Device Context	Select the firewalls to which the administrator can switch context for performing local configuration. If the list is long, you can filter by

Access Domain Settings	Description
(Corresponds to the Device/ Virtual Systems column in the Access Domain page)	**Device State**, **Platforms**, **Device Groups**, **Templates**, **Tags**, and **HA Status**.
Log Collector Groups	For each Collector Group you want to assign, **Add** and select it from the drop-down.

Panorama > Managed Devices > Summary

A Palo Alto Networks firewall that Panorama manages is called a *managed device*. Panorama can manage firewalls running the same major release or earlier major releases but Panorama cannot manage firewalls running a later major release. For example, Panorama running PAN-OS 10.0 can manage firewalls running PAN-OS 10.0 and earlier. Additionally, it is not recommended to manage firewalls running a later maintenance release than Panorama as this may result in features not working as expected. For example, it is not recommended to manage firewalls running PAN-OS 10.0.1 or later maintenance releases if Panorama is running PAN-OS 10.0.0. For more information on release information, see the PAN-OS 10.0 Release Notes. For more information on supported PAN-OS versions, see the End-of-Life Summary.

- Managed Firewall Administration
- Managed Firewall Information
- Firewall Software and Content Updates
- Firewall Backups

Managed Firewall Administration

You can perform the following administrative tasks on firewalls.

Task	Description
Add	**Add** firewalls and enter their serial numbers (one per row) to add them as managed devices. The **Managed Devices** window will then display Managed Firewall Information, including connection status, installed updates, and properties that were set during initial configuration. Check the **Associate Devices** box to associate the firewalls with a device group or template stack. **Import** multiple firewalls in CSV format to be managed by the Panorama management server. A sample CSV file is available for download. Next, enter the IP address of the Panorama management server on each firewall (see Device > Setup > Management) so that Panorama can manage the firewalls. *The firewall registers with Panorama over an SSL connection with AES-256 encryption. Panorama and the firewall authenticate each other using 2,048-bit certificates and use the SSL connection for configuration management and log collection.*
Reassociate	Reassign one or more selected firewalls to a different device group or template stack.
Delete	Select one or more firewalls and **Delete** them from the list of firewalls that Panorama manages.
Tag	Select one or more firewalls, click **Tag**, and enter a text string of up to 31 characters or select an existing tag. Do not use an empty space. Wherever the web interface displays a long list of firewalls (for example, in the dialog for installing software), tags provide one means to filter the list. For example, you can use a tag called branch office to filter for all branch office firewalls across your network.

Task	Description
Install	**Install** Firewall Software and Content Updates.
Group HA Peers	Select **Group HA Peers** if you want the **Managed Devices** page to group firewalls that are peers in a high availability (HA) configuration. You then can only select to perform actions on both peers or neither peer in each HA pair.
Manage (Backups)	**Manage** Firewall Backups.
PDF/CSV	Administrative roles with a minimum of read-only access can export the managed firewall table as **PDF/CSV**. You can apply filters to create more specific table configuration outputs for things such as audits. Only visible columns in the web interface will be exported. See Configuration Table Export.
Deploy Master Key	Deploy a new master key or update an existing master key of one or more devices.

Managed Firewall Information

Select **Panorama** > **Managed Devices** > **Summary** to display the following information for each managed firewall.

Managed Firewall Information	Description
Device Group	Displays the name of the device group in which the firewall is a member. By default, this column is hidden, though you can display it by selecting the drop-down in any column header and selecting **Columns** > **Device Group**. The page displays firewalls in clusters according to their device group. Each cluster has a header row that displays the device group name, the total number of assigned firewalls, the number of connected firewalls, and the device group path in the hierarchy. For example, **Data center (2/4 Devices Connected): Shared** > **Europe** > **Data center** would indicate that a device group named **Data center** has four member firewalls (two of which are connected) and is a child of a device group named **Europe**. You can collapse or expand any device group to hide or display its firewalls.
Device Name	Displays the hostname or serial number of the firewall. For the VM-Series NSX edition firewall, the firewall name appends the hostname of the ESXi host. For example, PA-VM: Host-NY5105
Virtual System	Lists the virtual systems available on a firewall that is in Multiple Virtual Systems mode.
Model	Displays the firewall model.
Tags	Displays the tags defined for each firewall/virtual system.

Managed Firewall Information	Description
Serial Number	Displays the serial number of the firewall.
Operational Mode	Displays the operational mode of the firewall. Can be FIPS-CC or Normal.
IP Address	Displays the IP address of the firewall/virtual system.
	IPv4—IPv4 address of the firewall/virtual system.
	IPv6—IPv6 address of the firewall/virtual system.
Variables	Create device specific variable definitions by copying them from a device in the template stack, or Edit existing variable definitions to create unique variables for the device. This column will be empty if the device is not associated with a template stack. By default, variables are inherited from the template stack. See Create or Edit Variable Definition on a Device.
Template	Displays the template stack to which the firewall is assigned.
Status	**Device State**—Indicates the state of the connection between Panorama and the firewall: Connected or Disconnected. A VM-Series firewall can have two additional states: • **Deactivated**—Indicates that you have deactivated a virtual machine either directly on the firewall or by selecting **Deactivate VMs** (**Panorama** > **Device Deployment** > **Licenses**) and removed all licenses and entitlements on the firewall. A deactivated firewall is no longer connected to Panorama because the deactivation process removes the serial number on the VM-Series firewall. • **Partially deactivated**—Indicates that you have initiated the license deactivation process from Panorama, but the process is not fully complete because the firewall is offline and Panorama cannot communicate with it.
	HA Status—Indicates whether the firewall is: • **Active**—Normal traffic-handling operational state • **Passive**—Normal backup state • **Initiating**—The firewall is in this state for up to 60 seconds after bootup • **Non-functional**—Error state • **Suspended**—An administrator disabled the firewall • **Tentative**—For a link or path monitoring event in an active/active configuration
	Shared Policy—Indicates whether the policy and object configurations on the firewall are synchronized with Panorama.
	Template—Indicates whether the network and device configurations on the firewall are synchronized with Panorama.

Managed Firewall Information	Description
Status (cont)	**Certificate**—Indicates the managed device's client certificate status. • **Pre-defined**—The managed device is using a pre-defined certificate to authenticate with Panorama. • **Deployed**—The custom certificate is successfully deployed on the managed device. • **Expires in N days N hours**—The currently installed certificate will expire in less than 30 days. • **Expires in N minutes**—The currently installed certificate will expire in less than one day. • **Client Identity Check Passed**—The certificate common name matches the serial number of the connecting device. • **OCSP Status Unknown**—Panorama cannot get the OCSP status from the OCSP responder. • **OCSP Status Unavailable**—Panorama cannot contact the OCSP responder. • **CRL Status Unknown**—Panorama cannot get the revocation status from the CRL database. • **CRL Status Unavailable**—Panorama cannot contact the CRL database.
	• **OCSP/CRL Status Unknown**—Panorama cannot get the OCSP or revocation status when both are enabled. • **OCSP/CRL Status Unavailable**—Panorama cannot contact the OCSP or CRL database when both are enabled. • **Untrusted Issuer**—The managed device has a custom certificate but the server is not validating it. **Last Commit State**—Indicates whether the last commit failed or succeeded on the firewall.
Software Version | Apps and Threat | Antivirus | URL Filtering | GlobalProtect™ Client | WildFire	Displays the software and content versions that are currently installed on the firewall. For details, see Firewall Software and Content Updates.
Backups	On each firewall commit, PAN-OS automatically sends a firewall configuration backup to Panorama. Click **Manage** to view the available configuration backups and optionally load one. For details, see Firewall Backups.
Last Master Key Push	Displays the status of the master key deployment from Panorama to the firewall.
	Status—Displays the latest master key push status. Can be `Success` or `Failed`. `Unknown` is displayed if a master key has not been pushed to the firewall from Panorama.
	Timestamp—Displays the date and time of the latest master key push from Panorama.

Managed Firewall Information	Description
Containers—If you deployed the CN-Series firewall to secure your containerized application workloads on Kubernetes clusters, use the following columns.	
Container Number of Nodes	Displays the number of containerized firewall data plane (CN-NGFW) that are connected to the Management plane (CN-Mgmt) registered to Panorama. The value can be 0—30 CN-NGFW pods for each pair of CN-Mgmt pods.
Container Notes	Future use

Create Device Variable Definition

When a device is first added to a template stack, you have the option to create device-specific variable definitions copied from devices in the template stack or you can edit the template variable definitions through **Panorama** > **Managed Devices** > **Summary**. By default, all variable definitions are inherited from the template stack and you can only override, and —not delete—the variable definitions for an individual device. You can use variables to replace IP address objects and IP address literals (IP Netmask, IP Range, FQDN) in all areas of the configuration, interfaces in the IKE Gateway configuration (Interface) and HA configuration (Group ID).

Create Device Variable Definition Information	Description
Clone device variable definition from another device in the template stack?	
No	View the existing variable definitions and edit as needed. See Panorama > Templates > Template Variables.
Yes	Select a device in the drop-down from which to clone variable definitions and then select the specific variable definitions you want to clone.

Firewall Software and Content Updates

To install a software or content update on a managed firewall, first use the **Panorama** > **Device Deployment** pages to download or upload the update to Panorama. Then select the **Panorama** > **Managed Devices** page, click **Install**, and complete the following fields.

To reduce traffic on the management (MGT) interface, you can configure Panorama to use a separate interface for deploying updates (see Panorama > Setup > Interfaces).

Firewall Software/Content Update Installation Options	Description
Type	Select the type of update you want to install: PAN-OS **Software**, **GlobalProtect Client** software, **Apps and Threats** signatures, **Antivirus** signatures, **WildFire**, or **URL Filtering**.
File	Select the update image. The drop-down includes only images that you downloaded or uploaded to Panorama using the **Panorama** > **Device Deployment** pages.
Filters	Select Filters to filter the Devices list.
Devices	Select the firewalls on which you want to install the image.
Device Name	The firewall name.
Current Version	The update version of the selected **Type** that is currently installed on the firewall.
HA Status	Indicates whether the firewall is: • **Active**—Normal traffic-handling operational state • **Passive**—Normal backup state • **Initiating**—The firewall is in this state for up to 60 seconds after bootup • **Non-functional**—Error state • **Suspended**—An administrator disabled the firewall • **Tentative**—For a link or path monitoring event in an active/active configuration
Group HA Peers	Select to group firewalls that are peers in a high availability (HA) configuration.
Filter Selected	If you want the Devices list to display only specific firewalls, select the corresponding device names and **Filter Selected**.
Upload only to device	Select to upload the image on the firewall but not automatically reboot the firewall. The image is installed when you manually reboot the firewall.
Reboot device after Install (Software only)	Select to upload and install the software image. The installation process triggers a reboot.
Disable new apps in content update (Apps and Threats only)	Select to disable applications in the update that are new relative to the last installed update. This protects against the latest threats while giving you the flexibility to enable applications after preparing any policy updates. Then, to enable applications, log in to the firewall, select **Device** > **Dynamic Updates**, click **Apps** in the Features column to display the new applications, and click **Enable/Disable** for each application you want to enable.

Firewall Backups

- Panorama > Managed Devices

Panorama automatically backs up every configuration change you commit to managed firewalls. To manage the backups for a firewall, select **Panorama** > **Managed Devices**, click **Manage** in the Backups column for the firewall, and perform any of the following tasks.

To configure the number of firewall configuration backups that Panorama stores, select Panorama > Setup > Management, edit the Logging and Reporting Settings, select Log Export and Reporting, and enter the Number of Versions for Config Backups (default is 100).

Task	Description
Display details about a saved or committed configuration.	In the Version column for the backup, click the saved configuration filename or committed configuration version number to display the contents of the associated XML file.
Restore a saved or committed configuration to the candidate configuration.	In the Action column for the backup, click **Load** and **Commit**. Loading a firewall configuration reverts the local device configuration and does not revert the configuration pushed from Panorama. After you **Load** the firewall backup, you must context switch to the firewall web interface or launch the firewall web interface to **Commit**.
Remove a saved configuration.	In the Action column for the saved backup, click Delete (✕).

Panorama > Device Quarantine

The **Panorama** > **Device Quarantine** page displays the devices that are in the quarantine list. Devices appear in this list as a result of the following actions:

- The system administrator added the device to this list manually.

  To manually **Add** a device, enter the **Host ID** and, optionally, the **Serial Number** of the device you need to quarantine.
- The system administrator selected the Host ID column from the Traffic, GlobalProtect, or Threat log, selected a device from that column, and then selected **Block Device**.
- The device matched a Security policy rule that has a log forwarding profile whose match list had a built-in action set to **Quarantine**.

  The Host ID displays in the GlobalProtect logs automatically. For the Host ID to display in the Traffic, Threat, or Unified logs, the Panorama appliance must have at least one security policy rule with the Source Device set to Quarantine. Without this setting in the security policy, Traffic, Threat or Unified logs will not have the Host ID, and the log forwarding profile will not take effect.
- The device was added to the quarantine list using an API.
- The Panorama appliance received the quarantine list as a part of redistributed entry (the quarantine list was redistributed from another Panorama appliance or firewall).

The Device Quarantine table includes the following fields.

Field	Description
Host ID	The Host-ID of the host that is blocked.
Reason	The reason that the device is quarantined. A reason of **Admin Add** means that an administrator manually added the device to the table.
Time Stamp	The time that the administrator or Security policy rule added the device to the quarantine list.
Source Device/App	The IP address of the Panorama, firewall, or third-party app that added the device to the quarantine list.
Serial Number	(Optional) The serial number of the quarantined device (if available).
User Name	(Optional) The username of the GlobalProtect client user who was logged in to the device when it was quarantined.

Panorama > Managed Devices > Health

Panorama™ allows you to monitor the hardware resources and performance for managed firewalls. Panorama centralizes time-trended performance information (CPU, memory, CPS, and throughput), logging performance, environmental information (such as fans, RAID status, and power supplies) and correlates events—such as commits, content installs, and software upgrades—to health data. When a firewall deviates from its calculated baseline, Panorama reports it as a Deviating Device to help identify, diagnose, and resolve any hardware issues quickly.

You can use this page to:

View Detailed Device Health.	View the health metrics of the devices managed by the Panorama.
Group HA Peers	View which firewalls are grouped together to help identify potential issues and determine if and which firewalls are impacted by any hardware resources or performance issues.
PDF/CSV	Administrative roles with a minimum of read-only access can export the managed firewall table in **PDF/CSV** format. You can apply filters to create more specific table-configuration outputs when needed, such as for audits. Only the visible columns in the web interface are exported. See Export Configuration Table Data.

Panorama > Managed Devices > Health > All Devices

Use this page to view the following information for each firewall.

Health Information	Description
Device Name	Hostname or serial number of the firewall. For the VM-Series NSX edition firewall, the firewall name appends the hostname of the ESXi host. For example, PA-VM: Host-NY5105
Model	Model of the firewall.
Device	
Throughput (Kilobits)	The data throughput over time (five-minute average) measured in kilobits per second.
CPS	Total connections per second for the firewall over time (five-minute average).
Session	
Counts (Sessions)	Total session count over time (five-minute average).
Data Plane	
CPU (%)	Total CPU utilization on the data plane.
Management Plane	
CPU (%)	Total CPU utilization on the management plane.
MEM (%)	Total memory utilization on the management plane.
Logging Rate (logs per second)	Rate at which the firewalls are forwarding logs to Panorama or a Log Collector (one-minute average).
Fans	Displays the presence, current status, RPM, and last failure of the fans in each fan tray. Fan status is displayed as *A*/*B*, where *A* is the number of good, running fans and *B* is the total number of fans on the firewall. Virtual firewalls display `N/A`.
Power Supplies	Displays the presence, current status, and last failure timestamps. Power supply status is displayed as *A*/*B*, where *A* is the number of good, running power supplies and *B* is the total number of power supplies on the device. Virtual firewalls display `N/A`.
Ports	Total number of ports in use on the firewall. Ports are displayed as *A*/*B*, where *A* is the number of good, running ports and *B* is the total number of ports on the device.

Panorama > Managed Devices > Health > Deviating Devices

The Deviating Devices tab displays devices that have any metrics that are deviating from their calculated baseline and displays those deviating metrics in red. A metric health baseline is determined by averaging the health performance for a given metric over seven days plus the standard deviation.

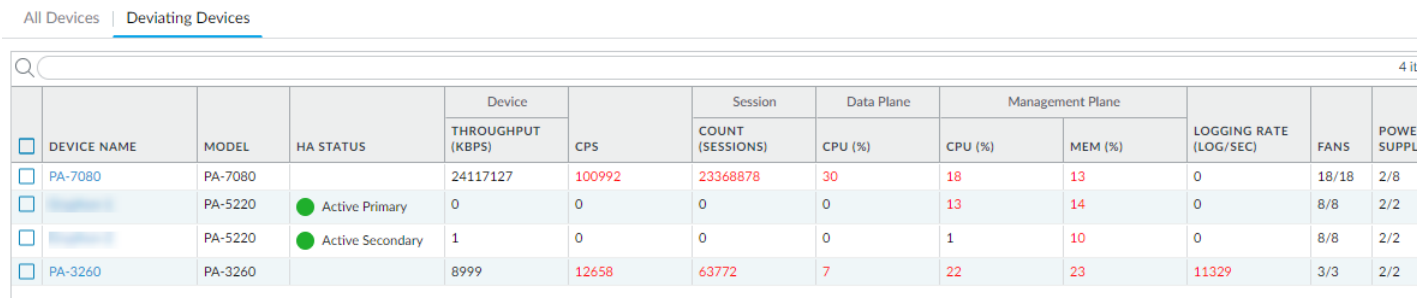


Figure 1: Example of a Deviated Metric

Detailed Device Health on Panorama

You can view a detailed device health history of an individual firewall by clicking the Device Name in either the All Devices tab or the Deviating Devices tab. The Detailed Device view provides the health status history using a time filter and displays the metadata associated with the device. Device health information is displayed as a table or as a widget where possible to provide a graphical representation of time-trended data.

Manage the Detailed Device View

Along with descriptive metadata associated with the firewall, the Detailed Device view displays the detailed firewall health information. Where applicable, you can configure Settings (⚙) for additional options for the widget or Maximize Panel (⛶) to enlarge the widget.

Field	Description
Actions	
Time Filter	Select the time filter to view the device health history from the drop-down. You can select **Last 12 hours**, **24 hours**, **7 days**, **15 days**, **30 days**, or **90 days**.
Show Average	Select the average and standard distribution shown on all time-trended widgets. You can select **None**, **Last 24 hours**, **7 days**, or **15 days**.
Refresh	Refresh displayed information with the latest data.
Print PDF	Generate a PDF of the currently displayed tab. *You need to have pop-ups enabled to select a download location and access the PDF.*
System Information	
System Information	The metadata associated with the device: IP address, software version, antivirus version, HA status, serial number, App and Threat version, Wildfire version, VSYS mode, model, and device mode.

Sessions

The Sessions tab displays the session information passing through the firewall. This information is displays as six individual graphs.

Field	Description
Throughput	The data throughput over time (five-minute average) measured in kilobits per second (Kbps).
Session Count	Total session count over time (five-minute average).
Connections per Second	Total CPS for the device over time (five-minute average).
Packets per Second	Total packets per second (averaged over five minutes) that passed through the device.
Global Session Table Utilization (PA-7000 and PA-5200 appliances only)	The percentage of the global session table over time for firewalls that have a global session table (averaged over five minutes).
Session Table Utilization	Shows the percentage of the session table usage for each dataplane for the firewall against time (averaged over five minutes).
SSL Decrypted Sessions Info	Shows the number of decrypted SSL sessions over time (averaged over five minutes).
SSL Proxy Session Utilization	Shows the utilization percentage of proxy sessions over time (averaged over five minutes).

Environments

The **Environments** tab displays the presence, status, and operating condition for hardware, such as power supplies, fan trays, and disk drives. This tab displays only for hardware-based firewalls:

Field	Description
Fan Status	Displays the presence, current status, RPM, and last failure of the fans in each fan tray. Fan status is displayed as *A*/*B*, where *A* is the number of good, running fans and *B* is the total number of fans on the firewall. Virtual firewalls display `N/A`.
Power Supply	Displays the presence, current status, and last failure timestamps. Power supply status is displayed as *A*/*B*, where *A* is the number of good, running power supplies and *B* is the total number of power supplies on the device. Virtual firewalls display `N/A`.
Thermal Status	Displays whether there are any thermal alarms associated with each slot of the device. If there is an active alarm, the firewall also displays more specific information here regarding exact temperature and location.

Field	Description
System Disk Status	Displays the available, used, and utilization percentage for the root, pancfg, panlogs, and panrepo mounts. System Disk Status also displays the disk name, size, and RAID status for firewalls that are RAID enabled.

Interfaces

The Interfaces tab displays the status and statistics across all physical interfaces on the firewall.

Field	Description
Interface Name	The name of the interface. Select an Interface to view graphs of the Bit Rate, Packets per Second, Errors, and Drops for the selected interface.
Status	The status of the interface: `AdminUp`, `Admin Down`, `OperationalUp`, or `Operational Down`.
Bit Rate	Displays the bit rate (bps) for received and transmitted data.
Packets per Second	Displays the packets per second for received and transmitted data.
Errors	Displays the number of errors for received and transmitted data.
Drops	Displays the number of dropped connections for received and transmitted data.

Logging

The Logging tab displays the logging rates and connections across manages firewalls.

Field	Description
Logging Rate	Displays the one-minute averaged rate for the device forwarding logs to Panorama or a Log Collector.
Logging Connections	Displays all available log forwarding connections, including their active or inactive status.
External Log Forwarding	Displays the sent, dropped, and average forwarding rate (logs per second) for various types of external log forwarding methods.

Resources

The Resources tab displays the CPU and memory statistics for the firewall.

Field	Description
Management Plane Memory	Displays the time-trended, five-minute average of the management plane memory as a percentage.
Packet Buffers	Displays the time-trended, five-minute average of the packet buffer utilization as a percentage. On a multiple dataplane system, this display includes different dataplanes, CPU, and packet buffers in different colors.
Packet Descriptors	Displays the time-trended, five-minute average of the packet descriptor utilization as a percentage. On a multiple dataplane system, this display includes different dataplanes, CPU, and packet buffers in different colors.
CPU Management Plane	Displays the time-trended, five-minute average of the management plane CPU.
CPU Data Plane	Displays the time-trended, five-minute average per-core utilization of the dataplane CPU. For systems with multiple data planes, you can select which dataplane to view selector.
Mounts	Displays the device system file info. This display includes the mount Name, Allocated (KB), Used (KB), and Avail (KB) space, as well as the Utilization percentage.

High Availability

The High Availability tab displays the HA status of the firewall and its HA peer. The top widget displays the configuration and content version of the device and its peers. The bottom widget provides information on the previous HA failovers and the reasons associated with it, including which firewall experienced the failure.

Panorama > Templates

Through the **Device** and **Network** tabs, you can deploy a common base configuration to multiple firewalls that require similar settings using a template or a template stack (a combination of templates). When managing firewall configurations with Panorama, you use a combination of device groups (to manage shared policies and objects) and templates (to manage shared device and network settings).

In addition to the settings available from the dialogs for creating Templates or Template Stacks, **Panorama** > **Templates** displays the following columns:

- **Type**—Identifies the listed entries as templates or template stacks.
- **Stack**—Lists the templates assigned to a template stack.

What do you want to do?	See:
Add, clone, edit, or delete a template	Templates
Add, clone, edit, or delete a template stack	Template Stacks
Looking for more?	Templates and Template Stacks
	Manage Templates and Template Stacks

Templates

Panorama supports up to 1,024 templates. You can **Add** a template and configure the settings as described in the following table. After creating a template, you need to also Configure a Template Stack and add the templates and firewalls to the template stack before you can manage your firewalls. After you configure a template, you must commit your changes in Panorama (see Panorama Commit Operations).

Deleting a template does not delete the values that Panorama pushed to the firewall.

Template Settings	Description
Name	Enter a template name (up to 31 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, periods, and underscores. In the **Device** and **Network** tabs, this name appears in the **Template** drop-down. The settings you modify in these tabs apply only to the selected **Template**.
Description	Enter a description for the template.

Template Stacks

You can configure a template stack or assign templates to a template stack. Assigning firewalls to a template stack allows you to push all necessary settings to the firewalls instead of adding every setting to every template individually. Panorama supports up to 1,024 stacks. You can **Add Stack** to create a new template

stack and configure the settings as described in the following table. After you configure a template stack, you must commit your changes in Panorama (see Panorama Commit Operations). Additionally, after you configure the network and device settings of firewalls assigned to the stack, you must perform a template commit and push the settings to the firewalls.

Deleting a template stack or removing a firewall from a template stack does not delete the values that Panorama previously pushed to that firewall; however, when you remove a firewall from a template stack, Panorama no longer pushes new updates to that firewall.

Template Stack Settings	Description
Name	Enter a stack name (up to 31 characters). The name is case-sensitive, must be unique, must start with a letter, and can contain only letters, numbers, and underscores. In the **Device** and **Network** tabs, the **Template** drop-down displays the stack name and its assigned templates.
Description	Enter a description for the stack.
Templates	**Add** each template you want to include in the stack (up to 8). If templates have duplicate settings, Panorama pushes only the settings from the template that is higher in the list when pushing settings to the assigned firewalls. For example, if Template_A is above Template_B in the list and both templates define the ethernet1/1 interface, then Panorama pushes the ethernet1/1 definition from Template_A and not from Template_B. To change the order of templates in the list, select a template and **Move Up** or **Move Down**. *Panorama doesn't validate template combinations in stacks so plan the order of your templates to avoid invalid relationships.*
Devices	Select each firewall that you want to add to the stack. If the list of firewalls is long, you can filter the list by **Platforms**, **Device Groups**, **Tags**, and **HA Status**. *You can assign firewalls that have non-matching modes (VPN mode, multiple virtual systems mode, or operational mode) to the same stack. Panorama pushes mode-specific settings only to those firewalls that support those modes.*
Select All	Selects every firewall in the list.
Deselect All	Deselects every firewall in the list.
Group HA Peers	Groups firewalls that are high availability (HA) peers. This enables you to easily identify firewalls that have an HA configuration. When pushing settings from the template stack, you can push to the grouped pair instead of to each firewall individually.
Filter Selected	To display only specific firewalls, select them and then **Filter Selected**.

Panorama > Templates > Template Variables

- New Template Variable Creation
- Edit Existing Template Variable
- Create or Edit Variable Definition on a Device

You can define variables (**Panorama** > **Templates**) for templates and template stacks or you can edit existing variables for an individual device (**Panorama** > **Managed Devices** > **Summary**). Variables are configuration components defined on the template or template stack that provide flexibility and re-usability when you use Panorama to manage firewall configurations. You can use variables to replace:

- An IP address (includes IP Netmask, IP Range, and FQDN) in all areas of the configuration.
- Interfaces in an IKE Gateway configuration (Interface) and in an HA configuration (Group ID).
- Configuration elements in your SD-WAN configuration (AS Number, QoS Profile, Egress Max, Link Tag).

When you add firewalls to a template stack, they automatically inherit variables that you create for a template or template stack.

Template Variable Information	Description
Name	The name of the variable definition.
Template (device and template stack)	Displays the name of the template to which the variable definition belongs.
Type	Displays the type of variable definition: • **IP Netmask**—Define a static IP or network address. • **IP Range**—Define an IP range. For example, 192.168.1.10-192.168.1.20. • **FQDN**—Define a fully qualified Domain Name. • **Group ID**—Define the High Availability Group ID. For more information, see Configuration Guidelines for Active/Passive HA. • **Device Priority—**Define the device priority to indicate a preference for which firewall should assume the active role in an Active-Passive high availability (HA) configuration. • **Device ID—**Define the Device ID to use to assign a device priority valuer in a Active-Active high availability (HA) configuration. • **Interface**—Define a firewall interface on the firewall. Can only be used for an IKE Gateway configuration. • **AS Number—**Define an autonomous system number to use in your BGP configuration. • **QoS Profile—**Define a Quality of Service (QoS) profile to use in QoS configurations. • **Egress Max—**Define an egress max value to use in QoS profile configuration. • **Link Tag—**Define a link tag to use in your SD-WAN configuration.
Value	Displays the configured value for the variable definition.
Add (template and template stack)	Add a new template variable definition.

Template Variable Information	Description
Delete	Delete an existing template variable definition.
Clone	Clone an existing template variable definition.
Override (template stack and device)	Overrides an existing template variable definition inherited from the template stack or device. You cannot change the variable type or name and you cannot override device-specific variables.
Revert (template stack and device)	To clear any overridden values on the template stack or device level; reverts the overridden variable to its original template variable definition.
Get values used on device only (device only)	Populate the selected variable with the value used on the firewall. Requires that a template or template stack variable be already defined and pushed to the firewall before Panorama can retrieve the value. Values fetched from the firewall will **Override** the template or template stack variable to create a device-specific variable. If no variable definition has been pushed to the firewall, Panorama will return `Value not found` for that variable.

New Template Variable Creation

Add a new template variable definition.

New Template Variable Definition Information	Description
Name	Name the variable definition. All variable definition names must start with the dollar sign (“$”) character.
Type	Select the type of variable definition: **IP Netmask**, **IP Range**, **FQDN**, **Group ID**, **Device Priority**, **Device ID**, **Interface**, **AS Number**, **QoS Profile**, **Egress Max**, or **Link Tag**.
Value	Enter the desired value for the variable definition.

Edit Existing Template Variable

You can edit a template variable definition for a template or template stack at any point after the variable is created (**Panorama** > **Templates**). **Manage** the template variables to select a variable and edit available values as needed.

Create or Edit Variable Definition on a Device

Go to **Panorama** > **Managed Devices** > **Summary** to create variable definitions or override template variables pushed from a Panorama template or template stack. Template variables include:

- An IP address (IP Netmask, IP Range, or FQDN) in all areas of the configuration.
- Interfaces in an IKE Gateway configuration (Interface) or an HA configuration (Group ID).
- Configuration elements in your SD-WAN configuration (AS Number, QoS Profile, Egress Max, Link Tag).

Creating a device variable allows you to copy overridden device-specific variables from a device in the same template stack instead of recreating them individually. By default, all variable definitions are inherited from the template or template stack and can be only overridden—you cannot delete or create new variable definitions for an individual device.

Create device variable definitions by copying variable definitions from existing devices in the template stack or **Edit** existing device variable definitions.

Panorama > Device Groups

Device groups comprise firewalls and virtual systems you want to manage as a group, such as the firewalls that manage a group of branch offices or individual departments in a company. Panorama treats these groups as single units when applying policies. Firewalls can belong to only one device group but, because virtual systems are distinct entities in Panorama, you can assign virtual systems within a firewall to different device groups.

You can nest device groups in a tree hierarchy of up to four levels under the Shared location to implement a layered approach for managing policies across your network of firewalls. At the bottom level, a device group can have parent, grandparent, and great-grandparent device groups at successively higher levels—collectively called *ancestors*—from which the bottom-level device group inherits policies and objects. At the top level, a device group can have child, grandchild, and great-grandchild device groups—collectively called *descendants*. When you select **Panorama** > **Device Groups**, the Name column displays this device group hierarchy.

After adding, editing, or deleting a device group, perform a Panorama commit and device group commit (see Panorama Commit Operations). Panorama then pushes the configuration changes to the firewalls that are assigned to the device group; Panorama supports up to 1,024 device groups.

To configure a device group, **Add** one and configure the settings as described in the following table.

Device Group Settings	Description
Name	Enter a name to identify the group (up to 31 characters). The name is case-sensitive, must be unique across the entire device group hierarchy, and can contain only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the device group.
Devices	Select each firewall that you want to add to the device group. If the list of firewalls is long, you can filter by **Device State**, **Platforms**, **Templates**, or **Tags**. The Filters section displays (in parentheses) the number of managed firewalls for each of these categories. If the purpose of a device group is purely organizational (that is, to contain other device groups), you don't need to assign firewalls to it.
Select All	Selects every firewall and virtual system in the list.
Deselect All	Deselects every firewall and virtual system in the list.
Group HA Peers	Select to group firewalls that are peers in a high availability (HA) configuration. The list then displays the active (or active-primary in an active/active configuration) firewall first and the passive (or active-secondary in an active/active configuration) firewall in parentheses. This enables you to easily identify firewalls that are in HA mode. When pushing shared policies, you can push to the grouped pair instead of individual peers.  *For HA peers in an active/passive configuration, consider adding both firewalls or their virtual systems to the same device group. This enables you to push the configuration to both peers simultaneously.*

Device Group Settings	Description
Filter Selected	If you want the Devices list to display only specific firewalls, select the firewalls and then **Filter Selected**.
Parent Device Group	Relative to the device group you are defining, select the device group (or the Shared location) that is just above it in the hierarchy (default is **Shared**).
Master Device	To configure policy rules and reports based on usernames and user groups, you must select a **Master Device**. This is the firewall from which Panorama receives usernames, user group names, and username-to-group mapping information.  *When you change the Master Device or set it to None, Panorama loses all the user and group information received from that firewall.*
Store users and groups from Master Device	This option displays only if you select a **Master Device**. The option enables Panorama to locally store usernames, user group names, and username-to-group mapping information that it receives from the **Master Device**. To enable local storage, you must also select **Panorama** > **Setup** > **Management**, edit the Panorama Settings, and Enable reporting and filtering on groups.
Dynamically Added Device Properties—When a new device is added to the device group, Panorama dynamically applies the specified authorization code and PAN-OS software version to the new device. This displays only after a device group is associated with an NSX service definition in Panorama.	
Authorization Code	Enter the authorization code to be applied to devices added to this device group.
SW Version	Select the software version to be applied to devices added to this device group.

Panorama > Managed Collectors

The Panorama management server (M-Series appliance or Panorama virtual appliance in Panorama mode) can manage Dedicated Log Collectors (M-Series appliances or Panorama virtual appliance in Log Collector mode). Each Panorama management server also has a local predefined Log Collector (named default) to process the logs it receives directly from firewalls. (A Panorama virtual appliance in Legacy mode stores the logs it receives directly from firewalls without using a Dedicated Log Collector.)

To use Panorama for managing a Dedicated Log Collector, add the Log Collector as a *managed collector*.

What do you want to do?	See:
Display Log Collector information	Log Collector Information
Add, edit, or delete a Log Collector	Log Collector Configuration
Update Panorama software on a Log Collector	Software Updates for Dedicated Log Collectors
Looking for more?	Centralized Logging and Reporting
	Configure a Managed Collector

Log Collector Information

Select **Panorama** > **Managed Collectors** to display the following information for Log Collectors. Additional parameters are configurable during Log Collector Configuration.

Log Collector Information	Description
Collector Name	The name that identifies this Log Collector. This name displays as the Log Collector hostname.
Serial Number	The serial number of the Panorama appliance that functions as the Log Collector. If the Log Collector is local, this is the serial number of the Panorama management server.
Software Version	The Panorama software release installed on the Log Collector.
IP Address	The IP address of the management interface on the Log Collector.
Connected	The status of the connection between the Log Collector and Panorama.
Configuration Status/Detail	Indicates whether the configuration on the Log Collector is synchronized with Panorama.
Run Time Status/ Detail	The status of the connection between this and other Log Collectors in the Collector Group.

Log Collector Information	Description
Log Redistribution State	Certain actions (for example, adding disks) will cause the Log Collector to redistribute the logs among its disk pairs. This column indicates the completion status of the redistribution process as a percentage.
Last Commit State	Indicates whether the last Collector Group commit performed on the Log Collector failed or succeeded.
Statistics	After you complete the Log Collector Configuration, click **Statistics** to view disk information, CPU performance, and the average log rate (logs/second). To better understand the log range you are reviewing, you can also view information on the oldest log that the Log Collector received.  *If you use an SNMP manager for centralized monitoring, you can also see loggings statistics in the panLogCollector MIB.*

Log Collector Configuration

Select **Panorama** > **Managed Collectors** to manage Log Collectors. When you **Add** a new Log Collector as a managed collector, the settings you configure vary based on the location of the Log Collector and whether you deployed Panorama in a high availability (HA) configuration:

- **Dedicated Log Collector**—When you add the Log Collector, initially the **Interfaces** tab doesn't display. You must enter the serial number (**Collector S/N**) of the Log Collector, click **OK**, and then edit the Log Collector to display the interface settings.
- **Default Log Collector that is local to the solitary (non-HA) or active (HA) Panorama management server**—After you enter the serial number (**Collector S/N**) of the Panorama management server, the Collector dialog displays only the **Disks**, **Communication** settings, and a subset of the **General** settings. The Log Collector derives its values for all other settings from the configuration of the Panorama management server.
- (HA only) **Default Log Collector that is local to the passive Panorama management server**—Panorama treats this Log Collector as remote so you must configure it as you would configure a Dedicated Log Collector.

 *The complete procedure to configure a Log Collector requires additional tasks.*

What are you looking for?	See:
Identify the Log Collector and define its connections to the Panorama management server and to external services.	General Log Collector Settings
Configure access to the Log Collector CLI.	Log Collector Authentication Settings
Configure the interfaces that the Dedicated Log Collector uses for	Log Collector Interface Settings

What are you looking for?	See:
management traffic, Collector Group communication, and log collection.	
Configure the RAID disks that store logs collected from firewalls.	Log Collector RAID Disk Settings
Configure the Log Collector to receive user mapping information from User-ID agents.	User-ID Agent Settings
Configure the Log Collector to authenticate with Windows User-ID Agents.	Connection Security
Configure security settings for communication with Panorama, other Log Collectors, and firewalls.	Communication Settings

General Log Collector Settings

- Panorama > Managed Collectors > General

Configure the settings as described in the following table to identify a Log Collector and define its connections to the Panorama management server, DNS servers, and NTP servers.

Log Collector General Settings	Description
Collector S/N	(Required) Enter the serial number of the Panorama appliance that functions as the Log Collector. If the Log Collector is local, enter the serial number of the Panorama management server.
Collector Name	Enter a name to identify this Log Collector (up to 31 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores. This name displays as the Log Collector hostname.
Inbound Certificate for Secure Syslog	Select the certificate that the managed collector must use to securely ingest logs from the Traps™ ESM server. This certificate is called an inbound certificate because the Panorama/ Managed Collector is the server to which the Traps ESM (client) is sending logs; the certificate is required if the **Transport** protocol for the log ingestion profile is **SSL**.
Certificate for Secure Syslog	Select a certificate for secure forwarding of syslogs to an external Syslog server. The certificate must have the **Certificate for Secure Syslog** option selected (see Manage Firewall and Panorama Certificates). When you assign a Syslog server profile to the Collector Group that includes this Log Collector (see Panorama > Collector Groups, **Panorama** > **Collector Groups** > **Collector Log Forwarding**), the **Transport** protocol of the server profile must be **SSL** (see Device > Server Profiles > Syslog).

Log Collector General Settings	Description
Panorama Server IP	Specify the IP address of the Panorama management server that manages this Log Collector.
Panorama Server IP 2	Specify the IP address of the secondary peer if the Panorama management server is deployed in a high availability (HA) configuration.
Domain	Enter the domain name of the Log Collector.
Primary DNS Server	Enter the IP address of the primary DNS server. The Log Collector uses this server for DNS queries (for example, to find the Panorama management server).
Secondary DNS Server	(Optional) Enter the IP address a secondary DNS server to use if the primary server is unavailable.
Primary NTP Server	Enter the IP address or host name of the primary NTP server, if any. If you do not use NTP servers, you can set the Log Collector time manually.
Secondary NTP Server	(Optional) Enter the IP address or host name of secondary NTP servers to use if the primary server is unavailable.
Timezone	Select the time zone of the Log Collector.
Latitude	Enter the latitude (-90.0 to 90.0) of the Log Collector. Traffic and threat maps use the latitude for App Scope.
Longitude	Enter the longitude (-180.0 to 180.0) of the Log Collector. Traffic and threat maps use the longitude for App Scope.

Log Collector Authentication Settings

- Panorama > Managed Collectors > Authentication

An M-Series appliance or Panorama virtual appliance in Log Collector mode (Dedicated Log Collector) does not have a web interface; only a CLI. You can use the Panorama management server to configure most settings on a Dedicated Log Collector but some settings require CLI access. To configure authentication settings for CLI access, configure the settings as described in the following table.

Log Collector Authentication Settings	Description
Authentication Profile	Select a configured authentication profile to define the authentication service that validates the login credentials of the Dedicated Log Collector or Panorama administrators.
Failed Attempts	Enter the number of failed login attempts that the Dedicated Log Collector allows on the CLI before locking out the administrator (range is 0 to 10; default is 10). Limiting login attempts helps protect the WildFire appliance from brute force attacks. A value of 0 specifies unlimited login attempts.

Log Collector Authentication Settings	Description
	*If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, then the administrator is indefinitely locked out until another administrator manually unlocks the locked-out administrator. If no other administrator has been created, you must reconfigure the Failed Attempts and Lockout Time settings on Panorama and push the configuration change to the Log Collector. To ensure that an administrator is never locked out, use the default (**0**) value for both Failed Attempts and Lockout Time.* *Set the number of Failed Attempts to 5 or fewer to accommodate a reasonable number of retries in case of typing errors, while preventing malicious systems from trying brute force methods to log in to the Dedicated Log Collector.*
Lockout Time (min)	Enter the number of minutes for which the Dedicated Log Collector locks out an administrator from access to the CLI after reaching the **Failed Attempts** limit (range is 0 to 60; default is 5). A value of 0 means the lockout applies until another administrator manually unlocks the account. *If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, then the administrator is indefinitely locked out until another administrator manually unlocks the locked-out administrator. If no other administrator has been created, you must reconfigure the Failed Attempts and Lockout Time settings on Panorama and push the configuration change to the Log Collector. To ensure that an administrator is never locked out, use the default (**0**) value for both Failed Attempts and Lockout Time.* *Set the Lockout Time to at least 30 minutes to prevent continuous login attempts from a malicious actor.*
Idle Timeout (min)	Enter the maximum number of minutes without any activity on the CLI before an administrator is automatically logged out (range is 0 to 1,440; default is None). A value of 0 means that inactivity does not trigger an automatic logout. *Set the Idle Timeout to 10 minutes to prevent unauthorized users from accessing the Dedicated Log Collector if an administrator leaves a session open.*
Max Session Count	Enter the number of active sessions the administrator can have open concurrently, The default is 0, which means that the Dedicated Log Collector can have an unlimited number of concurrently active sessions.
Max Session time	Enter the number of minutes the administrator can be logged in before being automatically logged out. The default is 0, which means that the administrator can be logged in indefinitely even if idle.

Log Collector Authentication Settings	Description
Local Administrators	Add and configure new administrators for the Dedicated Log Collector. These administrators are unique to the Dedicated Log Collector are managed from this page (**Panorama** > **Managed Collectors** > **Authentication**).
Panorama Administrators	Import existing administrators configured on Panorama. These administrators are created on Panorama and imported to the Dedicated Log Collector.

Log Collector Interface Settings

- Panorama > Managed Collectors > Interfaces

By default, Dedicated Log Collectors (M-Series appliances in Log Collector mode) use the management (MGT) interface for management traffic, log collection, and Collector Group communication. However, Palo Alto Networks recommends that you assign separate interfaces for log collection and Collector Group communication to reduce traffic on the MGT interface. You can improve security by defining a separate subnet for the MGT interface that is more private than the subnets for the other interfaces. To use separate interfaces, you must first configure them on the Panorama management server (see Device > Setup > Management). The interfaces that are available for log collection and Collector Group communication vary based on the Log Collector appliance model. For example, the M-500 appliance has the following interfaces: Ethernet1 (1Gbps), Ethernet2 (1Gbps), Ethernet3 (1Gbps), Ethernet4 (10Gbps), and Ethernet5 (10Gbps).

To configure an interface, select the link and configure the settings as described in the following table.

To complete the configuration of the MGT interface, you must specify the IP address, the netmask (for IPv4) or prefix length (for IPv6), and the default gateway. If you commit a partial configuration (for example, you might omit the default gateway), you can access the firewall or Panorama only through the console port for future configuration changes.

Always commit a complete MGT interface configuration. You cannot commit the configurations for other interfaces unless you specify the IP address, the netmask (for IPv4) or prefix length (for IPv6), and the default gateway.

Log Collector Interface Settings	Description
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	You must enable an interface to configure it. The exception is the MGT interface, which is enabled by default.
Speed and Duplex	Configure a data rate and duplex option for the interface. The choices include 10Mbps, 100Mbps, 1Gbps, and 10Gbps (Eth4 and Eth5 only) at full or half duplex. Use the default **auto-negotiate** setting to have the Log Collector determine the interface speed. *This setting must match the interface settings on the neighboring network equipment.*
IP Address (IPv4)	If your network uses IPv4 addresses, assign an IPv4 address to the interface.

Log Collector Interface Settings	Description
Netmask (IPv4)	If you assigned an IPv4 address to the interface, you must also enter a network mask (such as 255.255.255.0).
Default Gateway (IPv4)	If you assigned an IPv4 address to the interface, you must also assign an IPv4 address to the default gateway (the gateway must be on the same subnet as the MGT interface).
IPv6 Address/Prefix Length	If your network uses IPv6 addresses, assign an IPv6 address to the interface. To indicate the netmask, enter an IPv6 prefix length (such as 2001:400:f00::1/64).
Default IPv6 Gateway	If you assigned an IPv6 address to the interface, you must also assign an IPv6 address to the default gateway (the gateway must be on the same subnet as the interface).
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576 to 1,500; default is 1,500).
Device Log Collection	Enable the interface for collecting logs from firewalls. For a deployment with high log traffic, you can enable multiple interfaces to perform this function. This function is enabled by default on the MGT interface.
Collector Group Communication	Enable the interface for Collector Group communication (the default is the MGT interface). Only one interface can perform this function.
Syslog Forwarding	Enable the interface for forwarding syslogs (the default is the MGT interface). Only one interface can perform this function.
Network Connectivity Services	The **Ping** service is available on any interface and enables you to test connectivity between the Log Collector interface and external services. The following services are available only on the MGT interface: • **SSH**—Enables secure access to the Panorama CLI. • **SNMP**—Enables the interface to receive statistics queries from an SNMP manager. For details, see Enable SNMP Monitoring. • **User-ID**—Enables the Log Collector to redistribute user mapping information received from User-ID agents.
Permitted IP Addresses	Enter the IP addresses of the client systems that can access the Log Collector through this interface. An empty list (default) specifies that access is available to any client system. *Palo Alto Networks recommends that you do not leave this list blank; specify the client systems of Panorama administrators (only) to prevent unauthorized access.*

Log Collector RAID Disk Settings

- Panorama > Managed Collectors > Disks

After you configure logging disks on the M-Series appliance or Panorama virtual appliance, you can **Add** them to the Log Collector configuration.

By default, M-Series appliances are shipped with the first RAID 1 disk pair installed in bays A1 and A2. In the software, the disk pair in bays A1 and A2 is named Disk Pair A. The remaining bays are named sequentially: Disk Pair B, Disk Pair C, and so on. For example, the M-500 appliance supports up to 12 disk pairs. You can install pairs of 2TB or 1TB disks within the same appliance; however, disk size must be the same for both drives within each pair.

The Panorama virtual appliance supports up to 12 virtual logging disks for 24TB of storage capacity.

After you add disk pairs, the Log Collector redistributes its existing logs across all the disks, which can take hours for each terabyte of logs. During the redistribution process, the maximum log ingestion rate is reduced. In the **Panorama** > **Managed Collectors** page, the Log Redistribution State column indicates the completion status of the process as a percentage.

If you use an SNMP manager for centralized monitoring, you can see loggings statistics in the panLogCollector MIB.

User-ID Agent Settings

- Panorama > Managed Collectors > User-ID Agents

A Dedicated Log Collector can receive user mappings from up to 100 User-ID agents. The agents can be PAN-OS integrated User-ID agents that run on firewalls or Windows-based User-ID agents. On a firewall with multiple virtual systems, each virtual system can serve as a separate User-ID agent. The Log Collector can then redistribute the user mappings to firewalls or the Panorama management server.

The complete procedures to configure user mapping and enableusermapping redistributionrequire additional tasks besides connecting to User-ID agents.

To configure a Dedicated Log Collector to connect to a User-ID agent, **Add** one and configure the settings as described in the following table.

User-ID Agent Settings	Description
Name	Enter a name (up to 31 characters) to identify the User-ID agent. The name is case-sensitive, must be unique, and can contain only letters, numbers, spaces, hyphens, and underscores. *For a firewall serving as a User-ID agent, this field does not have to match the Collector Name field.*
Host	• **Windows-based User-ID agent**—Enter the IP address of the Windows host on which the User-ID agent is installed. • **Firewall (PAN-OS integrated User-ID agent)**—Enter the host name or IP address of the interface that the firewall uses to redistribute user mappings.
Port	Enter the port number on which the User-ID agent will listen for User-ID requests. The default is port 5007 but you can specify any available port. Different User-ID agents can use different ports.

User-ID Agent Settings	Description
	Some earlier versions of the User-ID agent use port 2010 as the default.
Collector Name	The collector that these fields refer to is the User-ID agent, not the Log Collector. The fields apply only if the agent is a firewall or virtual system that redistributes user mappings to the Log Collector. Enter the **Collector Name** and **Pre-Shared Key** that identify the firewall or virtual system as a User-ID agent. You must enter the same values as you did when configuring the firewall or virtual system to serve as a User-ID agent (see Redistribution).
Collector Pre-shared Key / Confirm Collector Pre-shared key	
Enabled	Select to enable the Log Collector to communicate with the User-ID agent.

Connection Security

- **Device** > **User Identification** > **Connection Security**
- **Panorama** > **User Identification** > **Connection Security**

To configure a certificate profile used by the Log Collector to validate the certificate presented by Windows User-ID agents. The Log Collector uses the selected certificate profile to verify the identity of the User-ID agent by validating the server certificate presented by the agent.

Task	Description
User-ID Certificate Profile	From the drop-down, select the certificate profile the firewall or Panorama uses to authenticate Windows User-ID agents or select **New Certificate Profile** to create one. Select **None** to remove the certificate profile.

Communication Settings

- Panorama > Managed Collectors > Communication

To configure custom certificate-based authentication between Log Collectors and Panorama, firewalls, and other Log Collectors, configure the settings as described in the following table.

Communication Settings	Description
Secure Server Communication—Enabling **Secure Server Communication** validates the identity of client devices connecting to the Log Collector.	
SSL/TLS Service Profile	Select a SSL/TLS service profile from the drop-down. This profile defines the certificate presented by the Log Collector and specifies the range of SSL/TLS versions acceptable for communication with the Log Collector.
Certificate Profile	Select a certificate profile from the drop-down. This certificate profile defines certificate revocation checking behavior and root CA used to authenticate the certificate chain presented by the client.

Communication Settings	Description
Custom Certificate Only	When enabled, the Log Collector only accepts custom certificates for authentication with managed firewalls and Log Collectors.
Authorize Clients Based on Serial Number	The Log Collector authorizes client devices based on uses a hash of their serial number.
Check Authorization List	Client devices or device groups connecting to this Log Collector are checked against the authorization list.
Disconnect Wait Time (min)	The amount of time the Log Collector waits before breaking the current connection with its managed devices. The Log Collector then reestablishes connections with its managed devices using the configured secure server communications settings. The wait time begins after the secure server communications configuration is committed.
Authorization List	**Authorization List**—Select Add and complete the following fields to set criteria. • **Identifier**—Select **Subject** or **Subject Alt. Name** as the authorization identifier. • **Type**—If Subject Alt. Name is selected as the Identifier, select **IP**, **hostname**, or **e-mail** as the type of the identifier. If Subject is selected, common-name is used as the identifier type. • **Value**—Enter the identifier value.
Secure Client Communication—Enabling **Secure Client Communication** ensures that the specified client certificate is used for authenticating the Log Collector over SSL connections with Panorama, firewalls, or other Log Collectors.	
Certificate Type	Select the type of device certificate (None, Local, or SCEP) used for securing communication
None	If **None** is selected, no device certificate is configured and the secure client communication is not used. This is the default selection.
Local	The Log Collector uses a local device certificate and the corresponding private key generated on the Log Collector or imported from an existing enterprise PKI server.
	Certificate—Select the local device certificate. This certificate can be a unique to the firewall (based on a hash of the Log Collector's serial number) or a common device certificate used by all Log Collectors connecting to Panorama.
	Certificate Profile—Select the Certificate Profile from the drop-down. This certificate profile is used for defining the server authentication with the Log Collector.
SCEP	The Log Collector uses a device certificate and private key generated Simple Certificate Enrollment Protocol (SCEP) server.
	SCEP Profile—Select a SCEP Profile from the drop-down.

Communication Settings	Description
	Certificate Profile— Select the Certificate Profile from the drop-down. This certificate profile is used for defining the server authentication with the Log Collector.
Check Server Identity	The client device confirms the server's identity by matching the common name (CN) with server's IP address or FQDN.

Software Updates for Dedicated Log Collectors

- Panorama > Managed Collectors

To install a software image on a Dedicated Log Collector, download or upload the image to Panorama (see Panorama > Device Deployment), click **Install** and complete the following fields.

Because the Panorama management server shares its operating system with the local default Log Collector, you upgrade both when installing a software update on the Panorama management server (see Panorama > Software).

For Dedicated Log Collectors, you can also select Panorama > Device Deployment > Software to install updates (see Manage Software and Content Updates).

To reduce traffic on the management (MGT) interface, you can configure Panorama to use a separate interface for deploying updates (see Panorama > Setup > Interfaces).

Fields to Install a Software Update on a Log Collector	Description
File	Select a downloaded or uploaded software image.
Devices	Select the Log Collectors on which to install the software. The dialog displays the following information for each Log Collector: • **Device Name**—The name of the Dedicated Log Collector. • **Current Version**—The Panorama software release currently installed on the Log Collector. • **HA Status**—This column does not apply to Log Collectors. Dedicated Log Collectors do not support high availability.
Filter Selected	To display only specific Log Collectors, select the Log Collectors and **Filter Selected**.
Upload only to device (do not Install)	Select to upload the software to the Log Collector without automatically rebooting it. The image is not installed until you manually reboot by logging into the Log Collector CLI and running the **`request restart system`** operational command.
Reboot device after Install	Select to upload and automatically install the software. The installation process reboots the Log Collector.

Panorama > Collector Groups

Each Collector Group can have up to 16 Log Collectors, to which you assign firewalls for forwarding logs. You can then use Panorama to query the Log Collectors for aggregated log viewing and investigation.

The predefined Collector Group named default contains the predefined Log Collector that is local to the Panorama management server.

Collector Group Configuration

To configure a Collector Group, click **Add** and complete the following fields.

Collector Group Settings	Configured In	Description
Name	**Panorama** > **Collector Groups** > **General**	Enter a name to identify this Collector Group (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Log Storage		Indicates the total storage quota for firewall logs that the Collector Group receives and the available space. Click the storage quota link to set the storage **Quota(%)** and expiration period (**Max Days**) for the following log types: • **Detailed Firewall Logs**—Includes all the log types in the **Device** > **Setup** > **Logging and Reporting Settings**, such as traffic, threat, HIP match, dynamically registered IP addresses (IP tag), extended PCAPs, GTP and Tunnel, App Stats, and more. • **Summary Firewall Logs**—Includes all the summary logs included in **Device** > **Setup** > **Logging and Reporting Settings**, such as traffic summary, threat summary, URL summary, and GTP and tunnel summary. • **Infrastructure and Audit Logs**—Includes the config, system, user-ID and authentication logs. • **Palo Alto Networks Platform Logs**—Includes logs from Traps and other Palo Alto Networks products. • **3rd Party External Logs**—Includes logs from other vendor integrations provided by Palo Alto Networks. To use the default settings, click **Restore Defaults**.
Min Retention Period (days)		Enter the minimum log retention period in days (1–2,000) that Panorama maintains across all Log Collectors in the Collector Group. If the current date minus the

Collector Group Settings	Configured In	Description
		date of the oldest log is less than the defined minimum retention period, Panorama generates a System log as an alert violation.
Collector Group Members		**Add** the Log Collectors that will be part of this Collector Group (up to 16). You can add any of the Log Collectors that are available in the **Panorama** > **Managed Collectors** page. All the Log Collectors for any particular Collector Group must be the same model: for example, all M-500 appliances or all Panorama virtual appliances. *After you add Log Collectors to an existing Collector Group, Panorama redistributes its existing logs across all the Log Collectors, which can take hours for each terabyte of logs. During the redistribution process, the maximum logging rate is reduced. In the Panorama > Collector Groups page, the Log Redistribution State column indicates the completion status of the process as a percentage.*
Enable log redundancy across collectors		If you select this option, each log in the Collector Group will have two copies and each copy will reside on a different Log Collector. This redundancy ensures that, if any one Log Collector becomes unavailable, no logs are lost: you can see all the logs forwarded to the Collector Group and run reports for all the log data. Log redundancy is available only if the Collector Group has multiple Log Collectors and each Log Collector has the same number of disks. In the **Panorama** > **Collector Groups** page, the Log Redistribution State column indicates the completion status of the process as a percentage. All the Log Collectors for any particular Collector Group must be the same model: for example, all M-500 appliances or all Panorama virtual appliances. *Because enabling redundancy creates more logs, this configuration requires more storage capacity. Enabling redundancy doubles the log processing traffic in a Collector Group, which reduces its maximum logging rate by half, as each Log Collector must distribute a copy of each log it receives. (When a Collector Group runs out of space, it deletes older logs.)*

Collector Group Settings	Configured In	Description
Forward to all collectors in the preference list		(PA-5200 Series and PA-7000 Series firewalls only) Select to send logs to every Log Collector in the preference list. Panorama uses round-robin load balancing to select which Log Collector receives the logs at any given moment. This is disabled by default: firewalls send logs only to the first Log Collector in the list unless that Log Collector becomes unavailable (see Devices / Collectors).
Enable Secure Inter LC Communication		Enables the use of custom certificates for mutual SSL authentication between Log Collectors in a Collector Group.
Location	**Panorama** > **Collector Groups** > **Monitoring**	Specify the location of the Collector Group.
Contact		Specify an email contact (for example, the email address of the SNMP administrator who will monitor the Log Collectors).
Version		Specify the SNMP version for communication with the Panorama management server: **V2c** or **V3**. SNMP enables you to collect information about Log Collectors, including connection status, disk drive statistics, software version, average CPU usage, average logs/second, and storage duration per log type. SNMP information is available on a per Collector Group basis.
SNMP Community String (V2c only)		Enter the **SNMP Community String**, which identifies a community of SNMP managers and monitored devices (Log Collectors, in this case), and serves as a password to authenticate the community members to each other. *Don't use the default community string public; it is well known and therefore not secure.*
Views (V3 only)		**Add** a group of SNMP views and, in **Views**, enter a name for the group. Each view is a paired object identifier (OID) and bitwise mask: the OID specifies a managed information base (MIB) and the mask (in hexadecimal format) specifies which SNMP objects are accessible within (include matching) or outside (exclude matching) that MIB. For each view in the group, **Add** the following settings: • **View**—Enter a name for a view. • **OID**—Enter the OID. • **Option** (include or exclude)—Choose whether the view will exclude or include the OID.

Collector Group Settings	Configured In	Description
		• **Mask**—Specify a mask value for a filter on the OID (for example, 0xf0).
Users (V3 only)		**Add** the following settings for each SNMP user: • **Users**—Enter a username for authenticating the user to the SNMP manager. • **View**—Select a group of views for the user. • **Authpwd**—Enter a password for authenticating the user to the SNMP manager (minimum eight characters). Only Secure Hash Algorithm (SHA) is supported for encrypting the password. • **Privpwd**—Enter a privacy password for encrypting SNMP messages to the SNMP manager (minimum eight characters). Only Advanced Encryption Standard (AES) is supported.
Devices / Collectors	**Panorama** > **Collector Groups** > **Device Log Forwarding**	The log forwarding preference list controls which firewalls forward logs to which Log Collectors. For each entry that you **Add** to the list, **Modify** the Devices list to assign one or more firewalls and **Add** one or more Log Collectors in the Collectors list. By default, the firewalls you assign in a list entry will send logs only to the primary (first) Log Collector as long as it is available. If the primary Log Collector fails, the firewalls send logs to the secondary Log Collector. If the secondary fails, the firewalls send logs to the tertiary Log Collector, and so on. To change the order, select a Log Collector and click **Move Up** or **Move Down**. *You can override the default log forwarding behavior for PA-5200 Series and PA-7000 Series firewalls by selecting* Forward to all collectors in the preference list *in the General tab.*
System Configuration HIP Match Traffic Threat WildFire Correlation	**Panorama** > **Collector Groups** > **Collector Log Forwarding**	For each type of firewall log that you want to forward from this Collector Group to external services, **Add** one or more match list profiles. The profiles specify which logs to forward and the destination servers. For each profile, complete the following: • **Name**—Enter a name of up to 31 characters to identify the match list profile. • **Filter**—By default, the firewall forwards **All Logs** of the type this match list profile applies to. To forward a subset of the logs, select an existing filter or select **Filter Builder** to add a new filter. For each query in a new filter, specify the following fields and **Add** the query:

Collector Group Settings	Configured In	Description
GTP Authentication User-ID Tunnel IP-Tag		• **Connector**—Select the connector logic (and/or). Select **Negate** if you want to apply negation. For example, to avoid forwarding logs from an untrusted zone, select **Negate**, select **Zone** as the Attribute, select **equal** as the Operator, and enter the name of the untrusted Zone in the Value column. • **Attribute**—Select a log attribute. The options vary by log type. • **Operator**—Select the criterion that determines how the attribute applies (such as **equal**). The options vary by log type. • **Value**—Specify the attribute value to match. To display or export the logs that the filter matches, select **View Filtered Logs**. This tab provides the same options as the **Monitoring** tab pages (such as **Monitoring** > **Logs** > **Traffic**). • **Description**—Enter a description of up to 1,023 characters to explain the purpose of this match list profile. • Destination servers—For each server type, **Add** one or more server profiles. To configure server profiles, see Device > Server Profiles > SNMP Trap, Device > Server Profiles > Syslog, Device > Server Profiles > Email, or Device > Server Profiles > HTTP. • Built-in Actions—You can **Add** actions for all log types except System and Configuration logs: • Enter a descriptive name for the **Action**. • Select the IP address you want to tag—**Source Address** or **Destination Address**. You can tag only the source IP address in Correlation logs and HIP Match logs. • Select the action—**Add Tag** or **Remove Tag**. • Select whether to register the tag with the local User-ID agent on this Panorama, or with a remote User-ID Agent. To register tags with a **Remote device User-ID Agent**, select the HTTP server profile that will enable forwarding. • Configure the IP-Tag **Timeout** to set, in minutes, the amount of time that IP address-to-tag mapping is maintained. Setting the timeout to 0 means that the IP-Tag mapping does not timeout (range is 0 to 43200 (30 days); default is 0). *You can only configure a timeout with the Add Tag action.*

Collector Group Settings	Configured In	Description
		• Enter or select the **Tags** you want to apply or remove from the target source or destination IP address.
Ingestion Profile	**Panorama** > **Collector Groups** > **Log Ingestion**	**Add** one or more log ingestion profiles that allow Panorama to receive logs from the Traps ESM server. To configure a new log ingestion profile, see Panorama > Log Ingestion Profile.

Collector Group Information

Select **Panorama** > **Collector Groups** to display the following information for Collector Groups. Additional fields are configurable after you complete the Log Collector Configuration.

Collector Group Information	Description
Name	A name that identifies the Collector Group.
Redundancy Enabled	Indicates whether log redundancy is enabled for the Collector Group. You can enable log redundancy for a collector group after you complete or modify the Log Collector Configuration.
Collectors	The Log Collectors assigned to the Collector Group.
Log Redistribution State	Certain actions (for example, enabling log redundancy) will cause the Collector Group to redistribute the logs among its Log Collectors. This column indicates the completion status of the redistribution process as a percentage.

Panorama > Plugins

- **Panorama** > **Plugins**
- **Device** > **Plugins**

Select **Panorama** > **Plugins** to install, remove, and manage the plugins that support third-party integrations on Panorama.

(Only available on the VM-Series firewalls) Select **Device** > **Plugins** to to install, remove, and manage the plugins for the VM-Series firewalls.

Plugins	Description
Upload	Allows you to upload a plug-in installation file from a local directory. This does not install the plugin. After uploading the installation file, the Install link becomes active.
File Name	The plug-in file name. When you install the **vm_series** plugin on Panorama, the **Device** > **VM-Series** page becomes available to you for managing and committing template configurations on the VM-Series firewalls deployed on the public cloud environments—AWS, Azure, and Google.
Version	The plug-in version number.
Platform	The models on which the plugin is supported.
Release date	The release date of this version of the plug-in.
Size	The plug-in file size.
Installed	Provides the current installation status of each plug-in on Panorama.
Actions	• **Install**—Installs the specified version of the plug-in. Installing a new version of the plug-in overwrites the previously installed version. • **Delete**—Deletes the specified plug-in file. • **Remove Config**—Removes all configuration related to the plug-in. To completely remove all configuration related to a plugin, you must also perform and **Uninstall** after using **Remove Config**. • **Uninstall**—Removes the current installation of the plug-in. This does not remove the plug-in file from Panorama. If you uninstall the plug-in, you lose any configuration related to that plug-in. Only use when completely removing the related configuration.

Panorama > SD-WAN

Download and install the Panorama SD-WAN plugin to centrally manage, monitor, and generate reports. Configure the SD-WAN topology from Panorama by adding and associating branches to their appropriate hubs, and associate those branch and hub devices to the appropriate zones. After configuring your SD-WAN topology, you can monitor the path health metrics across all configured devices and paths to isolate application and link issues, as well as understand your link performance over time. Additionally, you can generate reports for auditing purposes.

What do you want to do?	See:
Add, edit, or delete branch and hub devices	SD-WAN Devices
Add, edit, or delete a VPN cluster	SD-WAN VPN Clusters
Monitor path health	SD-WAN Monitoring
Generate health reports	SD-WAN Reports

SD-WAN Devices

- **Panorama** > **SD-WAN** > **Devices**

SD-WAN devices are branches or hubs that make up your VPN cluster and SD-WAN topology.

Field	Description
Name	Enter a name that identifies the SD-WAN device.
Type	Select the type of SD-WAN device: • **Hub**—A centralized firewall deployed at a primary office or location, such as a Data Center or business headquarters, that all branch devices connect to using a VPN connection. Traffic between branches passes through the hub before continuing to the target branch. Branches connect to hubs to gain access to centralized resources at the hub location. The hub device processes traffic, enforces policy rules, and manages link swapping at the primary office or location. • **Branch**—A firewall deployed at a physical branch location that connects to the hub using a VPN connection and provides security at the branch level. The branch connects to the hub for access to centralized resources. The branch device processes traffic, enforces policy rules, and manages link swapping at the branch location.
Virtual Router Name	Select the virtual router to use for routing between the SD-WAN hub and branches. By default, an `sdwan-default` virtual router is created and enables Panorama to automatically push router configurations.

Field	Description
Site	Enter a user-friendly site name that identifies the hub or branch. For example, enter the city name where the branch device is deployed.
Link Tag	(PAN-OS 10.0.3 and later 10.0 releases) For a hub, select the Link Tag that you created for a hub virtual interface so the hub can participate in DIA AnyPath. Auto VPN applies this link tag to the whole hub virtual interface, not an individual link. You reference this Link Tag in the Traffic Distribution Profile to indicate the order of failover to this hub virtual interface. On the branch device, Auto VPN uses this tag to populate the Link Tag field on the SD-WAN virtual interface that terminates on the hub device.
Zone Internet	**Add** one or more security zones to identify traffic going to and coming from untrusted sources.
Zone Hub	**Add** one or more security zones to identify traffic going to and coming from the SD-WAN hub devices.
Zone Branch	**Add** one or more security zones to identify traffic going to and coming from the SD-WAN branch devices.
Zone Internal	**Add** one or more security zones to identify traffic going to and coming from the trusted devices on the corporate network.
Router ID	Specify the BGP router ID. The Border Gateway Protocol (BGP) router ID must be unique between all routers.  *Use the Loopback Address as the Router ID.*
Loopback Address	Specify a static loopback IPv4 address for BGP peering.
AS Number	Enter the Autonomous System number to define a commonly defined routing policy to the internet. The AS number must unique for every hub and branch location.  *Use a 4-byte private BGP AS number to not interfere with any publicly routable AS number.*
Redistribution Profile Name	Select or create a redistribution profile to control which local prefixes are communicated to the hub router from the branch. By default, all locally connected internet prefixes are advertised to the hub location.  *Palo Alto Networks does not redistribute the branch office default route(s) learned from the ISP.*

SD-WAN VPN Clusters

- **Panorama** > **SD-WAN** > **VPN Clusters**

Associate SD-WAN branch devices with one or more SD-WAN hub devices to allow secure communication between the branch and hub locations. When you associate branch and hub devices in an SD-WAN VPN cluster, the firewall creates the required IKE and IPSec VPN connections between the sites based on the type of VPN cluster you specify.

Field	Description
Name	Enter a name that identifies the VPN cluster.
Type	Select the type of SD-WAN VPN cluster: • **Hub Spoke**—SD-WAN topology where a centralized firewall at a primary office or location acts as a gateway between branch devices connected using a VPN connection. Traffic between branches passes through the hub before continuing to the target branch.
Branches	**Add** one or more branch devices to associate with one or more hubs.
Hubs	**Add** one or more hub devices to associate with one or more branch devices. If multiple hubs are added, use path health quality metrics to control which is the primary hub and which are the secondary.

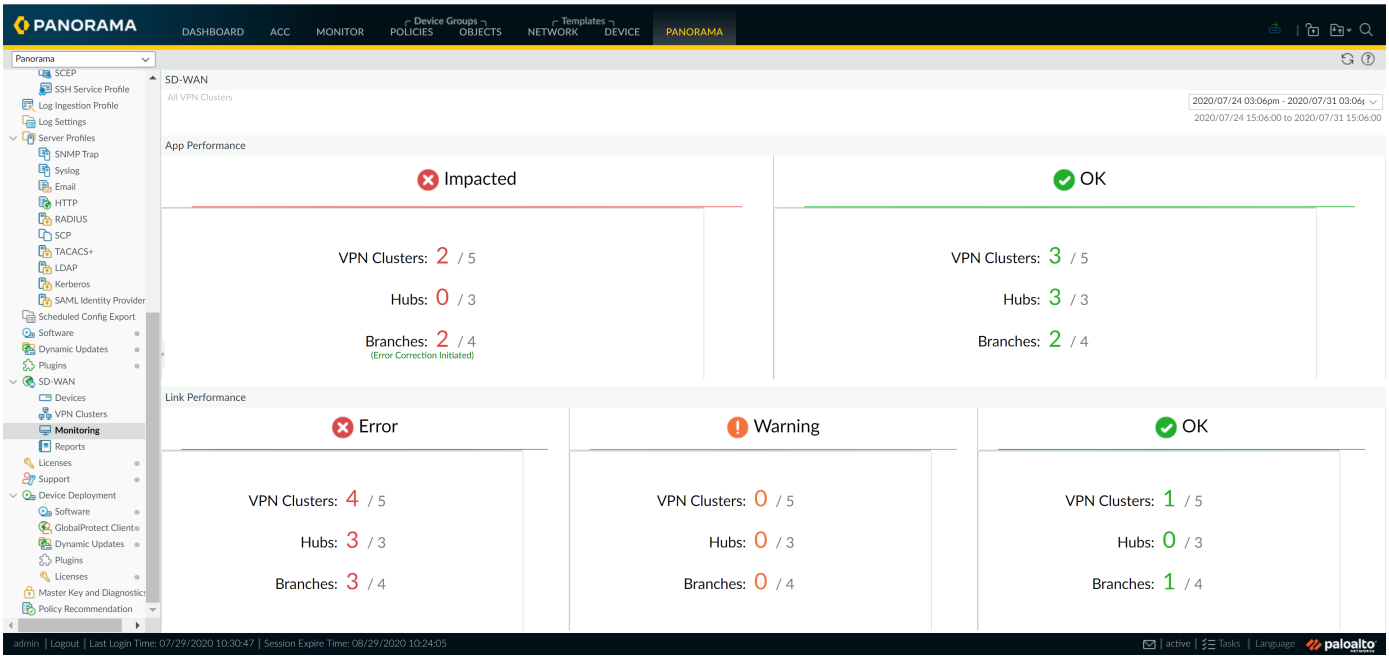
SD-WAN Monitoring

- **Panorama** > **SD-WAN** > **Monitoring**

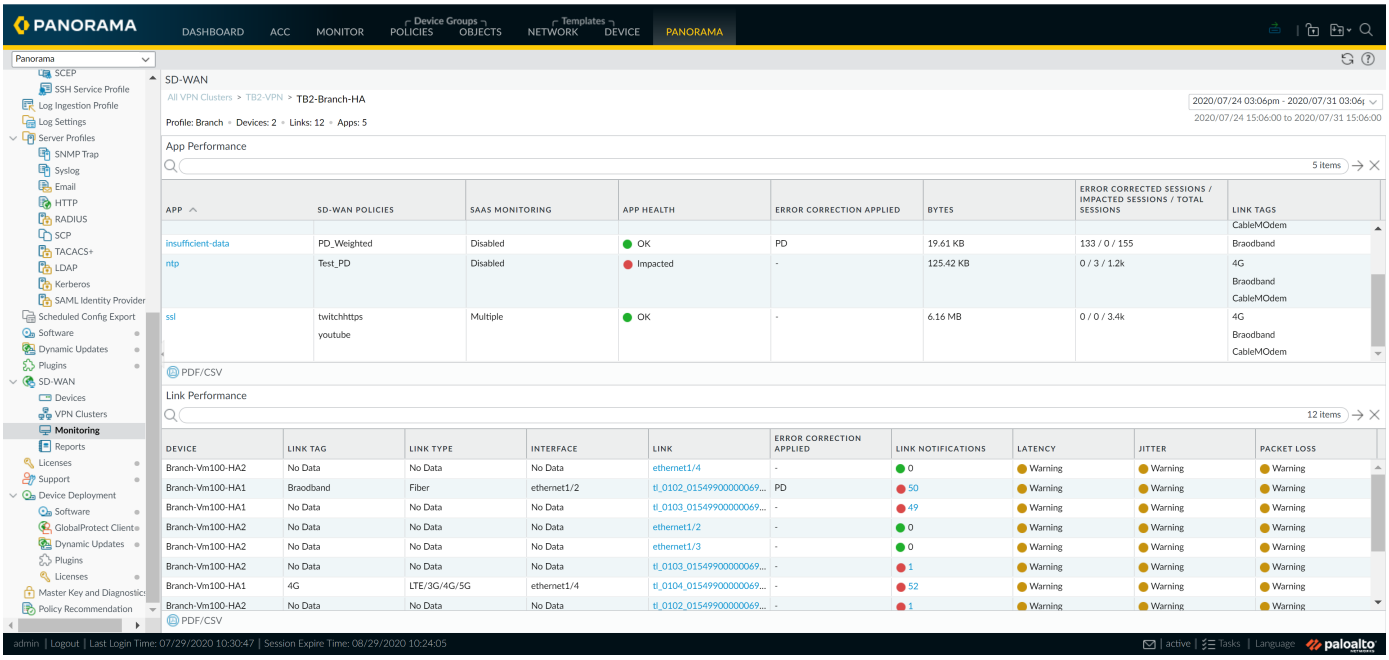
The Monitoring tab is a dashboard that displays a summary widgets of all your SD-WAN device health metrics. This tool provides actionable intelligence about the activity on your SD-WAN network, by allowing you to quickly identify applications or links experiencing performance issues. You can view path quality and link performance for all VPN Clusters, or for a specific VPN Cluster, within a specified period of time.

At a glance, you can view the total number of VPN Clusters with branch or hub firewalls that are experiencing impacted application performance, and those that are healthy. You can view the following application and link health states for VPN Clusters:

- App Performance
  - **Impacted**—One or more applications in the VPN Cluster for which none of the paths have jitter, latency, or packet loss performance at or below the specified thresholds in the Path Quality Profile in the list of paths that can be chosen.
  - **OK**—Applications in the VPN Cluster are healthy and experiencing no jitter, latency, or packet loss performance.
- Link Performance
  - **Error**—One or more sites in the VPN Cluster for which none of the paths have jitter, latency, or packet loss performance at or below the specified thresholds in the Path Quality Profile in the list of paths that can be chosen.
  - **Warning**—One or more Sites in the VPN Cluster have links with jitter, latency, or packet loss performance measurements that compare unfavorably to a moving seven day average value of the metric.
  - **OK**—Links in the VPN Cluster are healthy and experiencing no jitter, latency, or packet loss performance.



Click any widget to get an in-depth view of all VPN clusters for the desired health state. Additionally, you can use the Sites filter to view VPN clusters based on link notifications, latency deviations, jitter deviations, packet loss deviations, or impacted applications.



SD-WAN Reports

- **Panorama** > **SD-WAN** > **Reports**

Generate a report for application or link performance for the top applications or links that experienced the highest frequency of health degradation in the specified period of time for auditing purposes. After a report is configured, you must **Run Now** in order to view the report. Reports can be exported Functionality doesn't currently work. In what formats can reports be exported?

Field	Description
Name	Enter a name that identifies the purpose of the report.
Report Type	Select the type of report to run: • **App Performance**—Generate a report detailing the health metrics for all application traffic in the SD-WAN. • **Link Performance**—Generate a report detailing the health metrics for traffic across links in the SD-WAN.
Cluster	From the drop-down, select the cluster for which to generate a report. By default, **all** is selected.
Site	From the drop-down, select the site for which to generate a report. By default, **all** is selected. If **all** is selected for the Cluster, then you must generate a report for all sites attributed to the cluster. If a specific cluster is selected, then you may select a specific site for which to generate a report.
Application (App Performance Report Type only)	From the drop-down, select an application for which to generate a report. By default, **all** is selected. If **all** is selected for the Site, then you must generate a report for all applications attributed to the site. If a specific site is selected, then you may select a specific application for which to generate a report.
Link Tag (Link Performance Report Type only)	From the drop-down, select a link tag for which to generate a report. By default, **all** is selected. If **all** is selected for the Site, then you must generate a report for all link tags created under site. If a specific site is selected, then you may select a specific link tag for which to generate a report.
Link Type (Link Performance Report Type only)	From the drop-down, select a link type for which to generate a report. By default, **all** is selected. If **all** is selected for the Link Tag, then you must generate a report for all link types created under the Link Tag. If a specific Link Tag is selected, then you may select a specific link type for which to generate a report.
Top N	Specify the number of applications or links to include in the report. You may select that the report include the top 5, 10, 25, 50, 100, 250, 500, or 1000 performing applications or links. By default, **5** is selected.
Time Period	Set the time period for which to run the report. **None** is selected by default, which generates a report using all of the app and link performance data.

Panorama > VMware NSX

To automate the provisioning of a VM-Series NSX edition firewall, you must enable communication between the NSX Manager and Panorama. When Panorama registers the VM-Series firewall as a service on the NSX Manager, the NSX Manager has the configuration settings required to provision one or more instances of the VM#Series firewalls on each ESXi host in the cluster.

What do you want to know?	See:
How do I configure a Notify Group?	Configure a Notify Group
How do I define the configuration for the VM-Series NSX edition firewall?	Create Service Definitions
How do I configure Panorama to communicate with the NSX Manager?	Configure Access to the NSX Manager
How do I define steering rules for the VM-Series NSX edition firewall?	Create Steering Rules
How do I configure the firewall to consistently enforce policy in the dynamic vSphere environment?	Select Objects > Address Groups and Policies > Security To enable Panorama and the firewalls to learn about the changes in the virtual environment, use Dynamic Address Groups as source and destination address objects in Security policy pre rules.
Looking for more?	See Set up a VM-Series NSX Edition Firewall

Configure a Notify Group

- Panorama > Notify Group

The following table describes Panorama notify group settings.

Notify Group Settings	Description
Name	Enter a descriptive name for your notify group.
Notify Device	Check the boxes of the device groups that must be notified of additions or modifications to the virtual machines deployed on the network. As new virtual machines are provisioned or existing machines are modified, the changes in the virtual network are provided as updates to Panorama. When configured to do so, Panorama populates and updates the dynamic address objects referenced in policy rules so that the firewalls in the specified device groups receive changes to the registered IP addresses in the dynamic address groups.

Notify Group Settings	Description
	To enable notification, make sure to select every device group to which you want to enable notification. If you are not able to select a device group (no check box available), it means that the device group is automatically included by virtue of the device group hierarchy. This notification process creates context awareness and maintains application security on the network. If, for example, you have a group of hardware-based perimeter firewalls that must be notified when a new application or web server is deployed, this process initiates an automatic refresh of the dynamic address groups for the specified device group. And all policy rules that reference the dynamic address object now automatically include any newly deployed or modified application or web servers and can be securely enabled based on your criteria.

Create Service Definitions

- Panorama > VMware NSX > Service Definitions

A service definition allows you to register the VM-Series firewall as a partner security service on the NSX Manager. You can define up to 32 service definitions on Panorama and synchronize them on the NSX Manager.

Typically, you will create one service definition for each tenant in an ESXi cluster. Each service definition specifies the OVF (PAN-OS version) used to deploy the firewall and includes the configuration for the VM-Series firewalls installed on the ESXi cluster. To specify the configuration, a service definition must have a unique template, a unique device group and the license auth-codes for the firewalls that will be deployed using the service definition. When the firewall is deployed, it connects to Panorama and receives both its configuration settings—including the zone(s) for each tenant or department that the firewall will secure—and its policy settings from the device group specified in the service definition.

To add a new service definition, configure the settings as described in the following table.

Field	Description
Name	Enter the name for the service you want to display on the NSX Manager.
Description	(Optional) Enter a label to describe the purpose or function of this service definition.
Device Group	Select the device group or device group hierarchy to which these VM-Series firewalls will be assigned. For details, see Panorama > VMware NSX.
Template	Select the template to which the VM-Series firewalls will be assigned. For details, see Panorama > Templates. Each service definition must be assigned to a unique template or template stack. A template can have multiple zones (NSX Service Profile Zones for NSX) associated with it. For a single-tenant deployment, create one zone (NSX Service Profile Zone) in the template. If you have a multi-tenant deployment, create a zone for each sub-tenant. When you create a new NSX Service Profile Zone, it is automatically attached to a pair of virtual wire subinterfaces. For more information, see Network > Zones.

Field	Description
VM-Series OVF URL	Enter the URL (IP address or host name and path) where the NSX Manager can access the OVF file to provision new VM-Series firewalls.
Notify Groups	Select a notify group from the drop-down.

Configure Access to the NSX Manager

- Panorama > VMware NSX > Service Managers

To enable Panorama to communicate with the NSX Manager, **Add** and configure the settings as described in the following table.

Service Managers	Description
Service Manager Name	Enter a name to identify the VM-Series firewall as a service. This name displays on the NSX Manager and is used to deploy the VM-Series firewall on-demand. Supports up to 63 characters; use only letters, numbers, hyphens, and underscores.
Description	(Optional) Enter a label to describe the purpose or function of this service.
NSX Manager URL	Specify the URL that Panorama will use to establish a connection with the NSX Manager.
NSX Manager Login	Enter the authentication credentials—username and password—configured on the NSX Manager. Panorama uses these credentials to authenticate with the NSX Manager.
NSX Manager Password	
Confirm NSX Manager Password	
Service Definitions	Specify the service definitions associated with this service manager. Each service manager supports up to 32 service definitions.

After committing the changes to Panorama, the VMware Service Manager window displays the connection status between Panorama and the NSX Manager.

Sync Status	Description
Status	Displays the connection status between Panorama and the NSX Manager. A successful connection displays as Registered—Panorama and the NSX Manager are synchronized and the VM-Series firewall is registered as a service on the NSX Manager. For an unsuccessful connection, the status can be:

Sync Status	Description
	• **Connected Error**—Unable to reach/establish a network connection with the NSX Manager. • **Not authorized**—The access credentials (username and/or password) are incorrect. • **Unregistered**—The service manager, service definition, or service profile is unavailable or was deleted on the NSX Manager. • **Out of sync**—The configuration settings defined on Panorama are different from what is defined on the NSX Manager. Click **Out of sync** for details on the reasons for failure. For example, NSX Manager may have a service definition with the same name as defined on Panorama. To fix the error, use the service definition name listed in the error message to validate the service definition on the NSX Manager. Until the configuration on Panorama and the NSX Manager is synchronized, you cannot add a new service definition on Panorama.
Synchronize Dynamic Objects	Click **Synchronize Dynamic Objects** to refresh the dynamic object information from the NSX Manager. Synchronizing dynamic objects enables you to maintain context on changes in the virtual environment and allows you to safely enable applications by automatically updating the Dynamic Address Groups used in policy rules.  *On Panorama, you can view only the IP addresses that are dynamically registered from the NSX Manager. Panorama does not display the dynamic IP addresses that are registered directly to the firewalls. If you use VM Information Sources (not supported on the VM-Series NSX edition firewalls) or the XML API to register IP addresses dynamically to the firewalls, you must log in to each firewall to view the complete list of dynamic IP addresses (both those that Panorama pushed and those that are locally registered) on the firewall.*
NSX Config-Sync	Select **NSX Config-Sync** to synchronize the service definitions configured on Panorama with the NSX Manager. If you have any pending commits on Panorama, this option is not available. If the synchronization fails, view the details in the error message to know whether the error is on Panorama or on the NSX Manager. For example, when you delete a service definition on Panorama, the synchronization with the NSX Manager fails if the service definition is referenced in a rule on the NSX Manager. Use the information in the error message to determine the reason for failure and where you need to take corrective action (on Panorama or on the NSX Manager).

Create Steering Rules

- Panorama > VMware NSX > Steering Rules

Steering rules determine what traffic from which guests in the cluster is steered to the VM-Series firewall.

Field	Description
Auto-Generate Steering Rules	Generates steering rules based on a security rule that is configured as follows: • Belongs to a parent or a child device group registered with an NSX Service Manager.

Field	Description
	• Has the same zone as the source and destination (not any to any). • Has only one zone. • Has no static address group, IP range, or netmask configured for the policy. By default, steering rules generated through Panorama have no NSX Services configured and the NSX Traffic Direction is set to inout. After generating steering rules, you can update individual steering rules to change the NSX Traffic Direction or add NSX Services. Panorama automatically populates the following fields (except Description and NSX Services) when you auto-generate steering rules.
Name	Enter the name for the steering rule you want to display on the NSX Manager. When auto-generated, Panorama adds the prefix auto_ to each steering rule and replaces any space in the security policy rule name with an underscore (_).
Description	(Optional) Enter a label to describe the purpose or function of this service definition.
NSX Traffic Direction	Specify the direction of the traffic that is redirected to the VM-Series firewall. • **inout**—Creates an INOUT rule on NSX. Traffic of the specified type going between the source and the destination is redirected to the VM-Series firewall. Panorama uses this traffic direction for auto-generated steering rules. • **in**—Creates an IN rule on NSX. Traffic of the specified type going to the source from the destination is redirected to the VM-Series firewall. • **out**—Creates an OUT rule on NSX. Traffic of the specified type going from the source to the destination is redirected to the VM-Series firewall.
NSX Services	Select the application (Active Directory Server, HTTP, DNS, etc.) traffic to redirect to the VM-Series firewall.
Device Group	Select a device group from the drop-down. The chosen device group determines which security policies are applied to the steering rule. Device groups must be associated with an NSX service definition.
Security Policy	The security policy rule that the auto-generated steering rule is based on.

Panorama > Log Ingestion Profile

Use the log ingestion profile to enable Panorama to receive logs from external sources. In PAN-OS 8.0.0, Panorama (in Panorama mode) can serve as a Syslog receiver that can ingest logs from the Traps ESM server using Syslog. Support for new external log sources and the updates for newer Traps ESM versions will be pushed through content updates.

To enable log ingestion, you must configure Panorama as a Syslog receiver on the Traps ESM server, define a log ingestion profile on Panorama and attach the log ingestion profile to a Log Collector group.

To add a new external Syslog ingestion profile, **Add** a profile and configure the settings as described in the following table.

Field	Description
Name	Enter the name for the external Syslog ingestion profile. You can add up to 255 profiles.
Source Name	Enter the name or IP address of the external sources that will send logs. You can add up to 4 sources within a profile.
Port	Enter the port on which Panorama will be accessible over the network and will use to communicate and listen on. For Traps ESM, select a value between the range of 23000-23999. You must configure the same port number on the Traps ESM to enable communication between Panorama and the ESM.
Transport	Select TCP, UDP or SSL. If you select SSL, you must configure an inbound certificate for secure syslog communication in Panorama > Managed Collectors > General.
External Log Type	Select the log type from the drop-down.
Version	Select the version from the drop-down.

Use Monitor > External Logs to view information on the logs ingested from the Traps ESM server in to Panorama.

Panorama > Log Settings

Use the **Log Settings** page to forward the following log types to external services:

- System, Configuration, User-ID, and Correlation logs that the Panorama management server (M-Series appliance or Panorama virtual appliance in Panorama mode) generates locally.
- Logs of all types that the Panorama virtual appliance in Legacy mode generates locally or collects from firewalls.

For the logs that firewalls send to Log Collectors, complete the Log Collector Configuration *to enable forwarding to external services.*

Before starting, you must define server profiles for the external services (see Device > Server Profiles > SNMP Trap, Device > Server Profiles > Syslog, Device > Server Profiles > Email, and Device > Server Profiles > HTTP). Then **Add** one or more match list profiles and configure the settings as described in the following table.

Match List Profile Settings	Description
Name	Enter a name (up to 31 characters) to identify the match list profile.
Filter	By default, Panorama forwards **All Logs** of the type for which you are adding the match list profile. To forward a subset of the logs, open the drop-down and select an existing filter or select **Filter Builder** to add a new filter. For each query in a new filter, specify the following fields and **Add** the query: • **Connector**—Select the connector logic (and/or) for the query. Select **Negate** if you want to apply negation to the logic. For example, to avoid forwarding logs from an untrusted zone, select **Negate**, select **Zone** as the Attribute, select **equal** as the Operator, and enter the name of the untrusted Zone in the Value column. • **Attribute**—Select a log attribute. The options depend on the log type. • **Operator**—Select the criterion to determine whether the attribute applies (such as **equal**). The available options depend on the log type. • **Value**—Specify the attribute value for the query to match. To display or export the logs that the filter matches, select **View Filtered Logs**. This tab provides the same options as the **Monitoring** tab pages (such as **Monitoring** > **Logs** > **Traffic**).
Description	Enter a description of up to 1,024 characters to explain the purpose of this match list profile.
SNMP	**Add** one or more SNMP Trap server profiles to forward logs as SNMP traps (see Device > Server Profiles > SNMP Trap).
Email	**Add** one or more Email server profiles to forward logs as email notifications (see Device > Server Profiles > Email).
Syslog	**Add** one or more Syslog server profiles to forward logs as syslog messages (see Device > Server Profiles > Syslog).

Match List Profile Settings	Description
HTTP	**Add** one or more HTTP server profiles to forward logs as HTTP requests (see Device > Server Profiles > HTTP).
Built-in Actions	All log types except System logs and Configuration logs allow you to configure actions. • **Add** an action and enter a name to describe it. • Select the IP address you want to tag—**Source Address** or **Destination Address**. • Select the action—**Add Tag** or **Remove Tag**. • Select whether to distribute the tag to the local User-ID agent on this device, or to a remote User-ID Agent. • To distribute tags to a **Remote device User-ID Agent**, select the HTTP server profile that will enable forwarding. • Configure the IP-Tag **Timeout** to set, in minutes, the amount of time that IP address-to-tag mapping is maintained. Setting the timeout to 0 means that the IP-Tag mapping does not timeout (range is 0 to 43200 (30 days); default is 0). *You can only configure a timeout with the Add Tag action.* • Enter or select the **Tags** you want to apply or remove from the target source or destination IP address. You can tag the source IP address only, in Correlation logs and HIP Match logs.

Panorama > Server Profiles > SCP

- Panorama > Server Profiles > SCP

Select **Panorama** > **Server Profiles** > **SCP** to configure settings for the Secure Copy Protocol (SCP) server to securely copy and transfer files across your network so that you can automatically download and install content updates on managed firewalls, Log Collectors, and WildFire® appliances managed by an air-gapped Panorama™ management server.

SCP Server Settings	Description
Name	Enter a name to identify the server profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Server	Enter the server IP address or FQDN.
Port	Enter the server port for file transfer (range is 1–65,535; default is 22).
Username	Enter the username used to access the SCP server.
Password Confirm Password	Enter and confirm the case-sensitive password for the username used to access the SCP server.

Panorama > Scheduled Config Export

To schedule an export of all the running configurations on Panorama and firewalls, **Add** an export task and configure the settings as described in the following table.

If Panorama has a high availability (HA) configuration, you must perform these instructions on each peer to ensure the scheduled exports continue after a failover. Panorama does not synchronize scheduled configuration exports between HA peers.

Scheduled Configuration Export Settings	Description
Name	Enter a name to identify the configuration export job (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.
Description	Enter an optional description.
Enable	Select to enable the export job.
Scheduled export start time (daily)	Specify the time of day to start the export (24 hour clock, format HH:MM).
Protocol	Select the protocol to use to export logs from Panorama to a remote host. Secure Copy (**SCP**) is a secure protocol; **FTP** is not.
Hostname	Enter the IP address or hostname of the target SCP or FTP server.
Port	Enter the port number on the target server.
Path	Specify the path to the folder or directory on the target server that will store the exported configuration. For example, if the configuration bundle is stored in a folder called exported_config within a top level folder called Panorama, the syntax for each server type is: • SCP server: /Panorama/exported_config • FTP server: //Panorama/exported_config The following characters: **.**(period), **+**, **{** and **}**, **/**, **-**, _, **0**-**9**, **a**-**z**, and **A**-**Z**. Spaces are not supported in the file **Path**.
Enable FTP Passive Mode	Select to use FTP passive mode.
Username	Specify the username required to access the target system.
Password / Confirm Password	Specify the password required to access the target system. Use a password with maximum length of 15 characters. If the password exceeds 15 characters, the test SCP connection will display an error because the firewall encrypts the password when it tries to

Scheduled Configuration Export Settings	Description
	connect to the SCP server and the length of the encrypted password can be up to 63 characters only.
Test SCP server connection	Select to test communication between Panorama and the SCP host/server. To enable the secure transfer of data, you must verify and accept the host key of the SCP server. The connection is not established until the host key is accepted. If Panorama has an HA configuration, you must perform this verification on each HA peer so that each one accepts the host key of the SCP server.

Panorama > Software

Use this page to manage Panorama software updates on the Panorama management server.

- Manage Panorama Software Updates
- Display Panorama Software Update Information

Manage Panorama Software Updates

Select **Panorama** > **Software** to perform the tasks described in the following table.

By default, the Panorama management server saves up to two software updates. To make space for newer updates, the server automatically deletes the oldest update. You can change the number of software images that Panorama saves and manually delete images to free up space.

Refer to Install Content and Software Updates for Panorama for important information about version compatibility.

Task	Description
Check Now	If Panorama has access to the Internet, **Check Now** to display the latest update information (see Display Panorama Software Update Information). If Panorama does not have access to the external network, use a browser to visit the Software Update site for update information.
Upload	To upload a software image when Panorama does not have access to the Internet, use a browser to visit theSoftware Update site, locate the desired release and download the software image to a computer that Panorama can access, select **Panorama** > **Software**, click **Upload**, **Browse** to and select the software image, and click **OK**. When the upload is complete, the Downloaded column displays a check mark and the Action column displays **Install**.
Download	If Panorama has access to the Internet, **Download** (Action column) the desired release. When the download is complete, the Downloaded column displays a check mark.
Install	**Install** (Action column) the software image. When the installation finishes, Panorama logs you out while it reboots. *Panorama periodically performs a file system integrity check (FSCK) to prevent corruption of the Panorama system files. This check occurs after eight reboots or at a reboot that occurs 90 days after the last FSCK. A warning appears in the web interface and SSH login screens if an FSCK is in progress and you cannot log in until it completes. The time to complete this process varies by storage system size; for a large system, it can take several hours before you can log back into Panorama. To view progress, set up console access to Panorama.*

Task	Description
Release Notes	If Panorama has access to the Internet, you can access the **Release Notes** for the desired software release and review the release changes, fixes, known issues, compatibility issues, and changes to default behavior. If Panorama does not have access to the Internet, use a browser to visit the Software Update site and download the appropriate release.
	Deletes a software image when no longer needed or when you want to free up space for more images.

Display Panorama Software Update Information

Select **Panorama** > **Software** to display the following information. To display the latest information from Palo Alto Networks, click **Check Now**.

Software and Content Update Information	Description
Version	The Panorama software version
Size	The size in megabytes of the software image.
Release Date	The date and time when Palo Alto Networks made the update available.
Available	Indicates whether the image is available for installation.
Currently Installed	A check mark indicates that the update that is installed.
Action	Indicates the actions (**Download**, **Install**, or **Reinstall**) that are available for an image.
Release Notes	Click **Release Notes** to access the release notes for the desired software release and review the release changes, fixes, known issues, compatibility issues, and changes in default behavior.
	Deletes an update when no longer needed or to free up space for more downloads or uploads.

Panorama > Device Deployment

You can use Panorama to deploy software and content updates to multiple firewalls and Log Collectors and to manage firewall licenses.

What are you looking for?	See:
Deploy software and content updates to firewalls and Log Collectors.	Manage Software and Content Updates
See which software and content updates are installed or available for download and installation.	Display Software and Content Update Information
Schedule automatic content updates for firewalls and Log Collectors	Schedule Dynamic Content Updates
Revert the content versions of one or more firewalls from Panorama.	Revert Content Versions from Panorama
View, activate, deactivate, and refresh licenses. See the status of firewall licenses.	Manage Firewall Licenses
Looking for more?	Manage Licenses and Updates.

Manage Software and Content Updates

- Panorama > Device Deployment > Software

Panorama provides the following options for deploying software and content updates to firewalls and Log Collectors.

To reduce traffic on the management (MGT) interface, you can configure Panorama to use a separate interface for deploying updates (see Panorama > Setup > Interfaces).

Panorama Device Deployment Options	Description
Download	To deploy a software or content update when Panorama is connected to the Internet, **Download** the update. When the download finishes, the Available column displays Downloaded. You can then: • Install the PAN-OS/Panorama software update or content update. • Activate the GlobalProtect™ app or SSL VPN Client software update.

Panorama Device Deployment Options	Description
Upgrade	If a BrightCloud URL Filtering content update is available, click **Upgrade**. After a successful upgrade, you can Install the update on firewalls.
Install	After you Download or Upload a PAN-OS software, Panorama software, or content update, click **Install** in the Action column and select: • **Devices**—Select the firewalls or Log Collectors on which to install the update. If the list is long, use the Filters. Select **Group HA Peers** to group firewalls that are high availability (HA) peers. This enables you to easily identify firewalls that have an HA configuration. To display only specific firewalls or Log Collectors, select them and then **Filter Selected**. • **Upload only to device** (software only)—Select to load the software without automatically installing it. You must manually install the software. • **Reboot device after install** (software only)—Select to specify that the installation process automatically reboots the firewalls or Log Collectors. The installation cannot finish until a reboot occurs. • **Disable new apps in content update** (Applications and Threats only)—Select to disable applications in the update that are new relative to the last installed update. This protects against the latest threats while giving you the flexibility to enable applications after preparing any policy updates. Then, to enable applications, log in to the firewall, select **Device** > **Dynamic Updates**, click **Apps** in the Features column to display the new applications, and click **Enable/Disable** for each application you want to enable.  *You can also select Panorama > Managed Devices to install Firewall Software and Content Updates or Panorama > Managed Collectors to install Software Updates for Dedicated Log Collectors.*
Activate	After you Download or Upload a GlobalProtect app software update, click **Activate** in the Action column and select the options as follows: • **Devices**—Select the firewalls on which to activate the update. If the list is long, use the Filters. Select **Group HA Peers** to group firewalls that are high availability (HA) peers. This enables you to easily identify firewalls that have an HA configuration. To display only specific firewalls, select them and then **Filter Selected**. • **Upload only to device**—Select if you don't want PAN-OS to automatically activate the uploaded image. You must log in to the firewall and activate it.
Release Notes	Click **Release Notes** to access the release notes for the desired software release and review the release changes, fixes, known issues, compatibility issues, and changes in default behavior.
Documentation	Click **Documentation** to access the release notes for the desired content release.
	Deletes software or content updates when no longer needed or when you want to free up space for more downloads or uploads.
Check Now	**Check Now** to Display Software and Content Update Information.

Panorama Device Deployment Options	Description
Upload	To deploy a software or content update when Panorama is not connected to the Internet, download the update to your computer from the Software Updates or Dynamic Updates site, select the **Panorama** > **Device Deployment** page that corresponds to the update type, click **Upload**, select the update **Type** (content updates only), select the uploaded file, and click **OK**. The steps to then install or activate the update depend on the type: • **PAN-OS or Panorama software**—When the upload is complete, the Downloaded column displays check mark and you can the Action column displays **Install**. • **GlobalProtect Client or SSL VPN Client software**—Activate from file. • **Dynamic updates**—Install from file.
Install from File	After you upload a content update, click **Install from File**, select the content **Type**, select the filename of the update, and select the firewalls or Log Collectors.
Activate from File	After you upload a GlobalProtect app software update, click **Activate from File**, select the filename of the update, and select the firewalls.
Schedules	Select to Schedule Dynamic Content Updates.

Display Software and Content Update Information

- Panorama > Device Deployment > Software

Select **Panorama** > **Device Deployment** > **Software** to display PAN-OS **Software**, **GlobalProtect Client** software, and **Dynamic Updates** (content) that are currently installed or available for download and installation. The **Dynamic Updates** page organizes the information by content type (Antivirus, Applications and Threats, URL Filtering, and WildFire) and indicates the date and time of the last check for updated information. To display the latest software or content information from Palo Alto Networks, click **Check Now**.

Software and Content Update Information	
Version	The software or content update version.
File Name	The name of the update file.
Platform	The designated firewall or Log Collector model for the update. A number indicates a hardware firewall model (for example, `7000` indicates the PA-7000 Series firewall), `vm` indicates the VM-Series firewall, and `m` indicates the M-Series appliance.
Features	(Content only) Lists the type of signatures the content version might include.
Type	(Content only) Indicates whether the download includes a full database update or an incremental update.
Size	The size of the update file.

Software and Content Update Information	
Release Date	The date and time when Palo Alto Networks made the update available.
Available	(PAN-OS or Panorama software only) Indicates that the update is downloaded or uploaded.
Downloaded	(SSL VPN Client software, GlobalProtect Client software, or content only) A check mark indicates that the update is downloaded.
Action	Indicates the action you can perform on the update: Download, Upgrade, Install or Activate.
Documentation	(Content only) Provides a link to the release notes for the desired content release.
Release Notes	(Software only) Provides a link to the release notes for the desired software release.
	Deletes an update when no longer needed or when you want to free up space for more downloads or uploads.

Schedule Dynamic Content Updates

- Panorama > Device Deployment > Dynamic Updates

To schedule an automatic download and installation of an update, click **Schedules**, click **Add**, and configure the settings as described in the following table.

Dynamic Update Schedule Settings	
Name	Enter a name to identify the scheduled job (up to 31 characters). The name is case-sensitive, must be unique, and can contain only letters, numbers, hyphens, and underscores.
Disabled	Select to disable the scheduled job.
Download Source	Select the download source for the content update. You can select to download content updates from the Palo Alto Networks **Updates Server** or from an **SCP** server.
SCP Profile (SCP only)	Select a configured SCP profile from which to download.
SCP Path (SCP only)	Enter the specific path on the SCP server from which to download the content update.
Type	Select the type of content update to schedule: **App**, **App and Threat**, **Antivirus**, **WildFire**, or **URL Database**.
Recurrence	Select the interval at which Panorama checks in with the update server. The recurrence options vary by update type.
Time	For a **Daily** update, select the **Time** from the 24-hour clock.

Dynamic Update Schedule Settings	
	For a **Weekly** update, select the **Day** of week, and the **Time** from the 24-hour clock.
Disable new apps in content update	You can disable new apps in content updates only if you set the update **Type** to **App** or **App and Threat** and only if **Action** is set to **Download and Install**. Select to disable applications in the update that are new relative to the last installed update. This protects against the latest threats while giving you the flexibility to enable the applications after preparing any policy updates. Then, to enable applications, log in to the firewall, select **Device** > **Dynamic Updates**, click **Apps** in the Features column to display the new applications, and click **Enable/Disable** for each application you want to enable.
Action	• **Download Only**—Panorama™ will download the scheduled update. You must manually install the update on firewalls and Log Collectors. • **Download and Install**—Panorama will download and automatically install the scheduled update. • **Download and SCP**—Panorama will download and transfer the content update package to the specified SCP server.
Devices	Select **Devices** and then select the firewalls that will receive scheduled content updates.
Log Collectors	Select **Log Collectors** and then select the managed collectors that will receive scheduled content updates.

Revert Content Versions from Panorama

- Panorama > Device Deployment > Dynamic Updates

Quickly **Revert Content** version of the Applications, Applications and Threats, Antivirus, WildFire and WildFire content updates of one or more firewalls to the previously installed content version from Panorama. The content version you are reverting to must be an older version than the one currently installed on the firewall. Reverting content is available on Panorama running 8.1. Content on firewalls can be reverted so long as the revert function is available locally on the firewall.

Field	Description
Filter	Filter which devices you would like to revert content. You can filter by: • Device State • Platforms • Device Groups • Templates • Tags • HA Status • Software Version (PAN-OS) • Current Content Version
Devices	Select one or more devices to revert. Displays the following devices information:

Field	Description
	• Device Name—The name of the firewall. • Current version—Current content version installed on the device. Column will show 0 if no content version is installed. • Previous version (content)—The previously installed content version on the firewalls running PAN 8.1 or later. Column will be blank if no content version was previously installed or if the firewall is running a PAN-OS version prior to 8.1 • Software Version—The current PAN-OS version installed on the device. • HA Status—Displays HA status when an in HA pair. Column will be blank if the device is not in an HA pair.
Group HA pairs	Check this box to group HA peers.

Once you have selected the devices to revert, click **OK**.

Manage Firewall Licenses

- Panorama > Device Deployment > Licenses

Select **Panorama** > **Device Deployment** > **Licenses** to perform the following tasks:

- Update licenses of firewalls that don't have direct internet access—Click Refresh.
- Activate a license on firewalls—To activate a license on firewalls, click **Activate**, select the firewalls and, in the Auth Code column, enter the authorization codes that Palo Alto Networks provided for the firewalls.
- Deactivate all the licenses and subscriptions/entitlements installed on VM-Series firewalls—Click **Deactivate VMs**, select the firewalls (the list displays only firewalls running PAN-OS 7.0 or later releases), and click:
  - **Continue**—Deactivates the licenses and automatically registers the changes with the licensing server. The licenses are credited back to your account and are available for reuse.
  - **Complete Manually**—Generates a token file. Use this if Panorama does not have direct Internet access. To complete the deactivation process, you must log in to the Support portal, select **Assets**, click **Deactivate License(s)**, upload the token file, and click **Submit**. After you complete the deactivation process.

You can also view the current license status for managed firewalls. For firewalls that have direct internet access, Panorama automatically performs a daily check-in with the licensing server, retrieves license updates and renewals, and pushes them to the firewalls. The check-in is hard-coded to occur between 1 and 2 A.M.; you cannot change this schedule.

Firewall License Information	
Device	The firewall name.
Virtual System	Indicates whether the firewall does ✓ or does not ⊗ support multiple virtual systems.

Firewall License Information	
Threat Prevention	Indicates whether the license is active, inactive, or expired (along with the expiration date).
URL	
Support	
GlobalProtect Gateway	
GlobalProtect Portal	
WildFire	
VM-Series Capacity	Indicates whether this is or is not a VM-Series firewall.