Palo Alto Networks

Web Interface Reference Guide
Version 7.0

Contact Information

Corporate Headquarters:

Palo Alto Networks

4401 Great America Parkway

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-us

About this Guide

This guide describes the Palo Alto Networks next-generation firewall and Panorama™ web interfaces. It provides information on how to use the web interface and reference information about how to populate fields within the interface:

- For information on the additional capabilities and for instructions on configuring the features on the firewall, refer to https://www.paloaltonetworks.com/documentation.
- For access to the knowledge base, complete documentation set, discussion forums, and videos, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.
- For the most current PAN-OS and Panorama 7.0 release notes, go to https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os-release-notes.html.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: February 18, 2016

Table of Contents

Chapter 1

Chapter 2

Chapter 3

Chapter 5

Chapter 6

Chapter 1
Introduction

This section provides an overview of the firewall:

- "Firewall Overview"
- "Features and Benefits"
- "Management Interfaces"

Firewall Overview

Palo Alto Networks® offers a full line of next-generation security appliances that range from the PA-200 firewall, designed for enterprise remote offices, to a PA-7000 Series firewall, which is a modular chassis designed for high-speed data centers. The firewall allows you to specify security policies based on accurate identification of each application that will traverse your network. Unlike traditional firewalls that identify applications only by protocol and port number, the Palo Alto Networks next-generation firewall uses packet inspection and a library of application signatures to distinguish between applications that have the same protocol and port and to identify potentially malicious applications that use nonstandard ports.

In order to safely enable the use of applications, maintain complete visibility and control, and protect the organization from the latest cyber threat, you can define security policies for specific applications or application groups rather than using a single policy for all port 80 connections. For each identified application, you can specify a security policy to block or allow traffic based on the source and destination zones and addresses (IPv4 and IPv6). Each security policy can also specify security profiles to protect against viruses, spyware, and other threats.

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 "Configuring the Firewall for 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 "Security Profiles").

- **URL filtering**—Outbound connections can be filtered to prevent access to inappropriate web sites (see "URL Filtering Profiles").

- **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 "Reports and Logs").

- **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 "Enabling HA on the Firewall").

- **Malware analysis and reporting**—The WildFire™ security service provides detailed analysis and reporting on malware that passes through the firewall.

- **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 devices through the Panorama centralized management system, which has a web interface very similar to the web interface on Palo Alto Networks firewalls.

Management Interfaces

Palo Alto Networks next-generation firewalls support the following management interfaces.

- **Web interface**—Configuration and monitoring over HTTP or HTTPS from a web browser.
- **CLI**—Text-based configuration and monitoring over Telnet, Secure Shell (SSH), or the console port.
- **Panorama—**Palo Alto Networks product that provides web-based management, reporting, and logging for multiple firewalls. The Panorama interface is similar to the firewall web interface but with additional management functions (see "Central Device Management Using Panorama" for information on using Panorama).
- **XML API—**Provides a Representational State Transfer (REST)-based interface to access device configuration, operational status, reports, and packet captures from the firewall. There is an API browser available on the firewall at *https://<firewall>/api*, where *<firewall>* is the host name or IP address of the firewall. This link provides help on the parameters required for each type of API call.

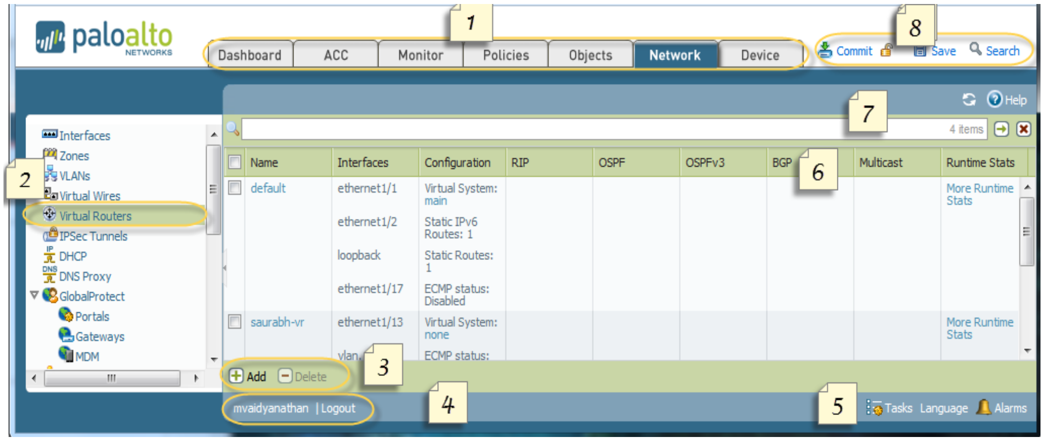
Chapter 2

Getting Started

This chapter describes how to set up and start using your Palo Alto Networks® firewall:

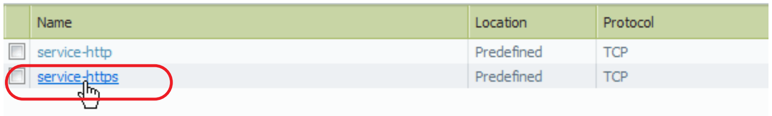
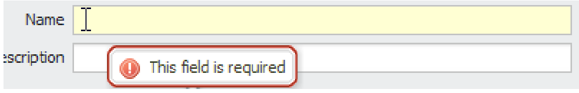
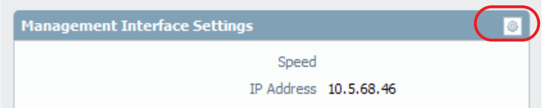
- "Using the Palo Alto Networks Firewall Web Interface"
- "Getting Help Configuring the Firewall"

Using the Palo Alto Networks Firewall Web Interface



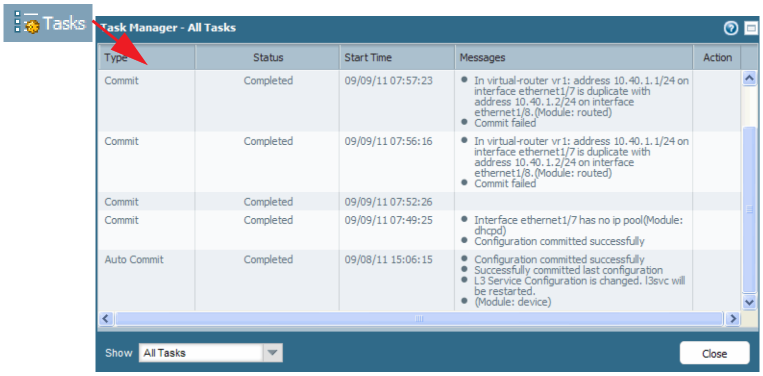
Name	Interfaces	Configuration	RIP	OSPF	OSPFv3	BGP	Multicast	Runtime Stats
default	ethernet1/1 ethernet1/2 loopback ethernet1/17	Virtual System: main Static IPv6 Routes: 1 Static Routes: 1 ECMP status: Disabled						More Runtime Stats
saurabh-vr	ethernet1/13 vlan.	Virtual System: none ECMP status:						More Runtime Stats

Item	Description
1	Click the tab along the top to view the configuration items under the category. The highlighted item is selected.
2	Select an option from the left pane to view the options within a tab. For example, in the screenshot above the **Virtual Routers** pane is selected in the **Network** tab. This document identifies this navigation path in the web interface as **Network > Virtual Routers**. For some tabs, the configuration options are nested. Click the ▷ drop-down on the left pane to expand and collapse the configuration options included within the pane.

Item	Description
3	The action buttons vary by page but most pages include the following buttons: • **Add**—Click **Add** to create a new item. • **Delete**—To delete one or more items, select the check boxes next to the item and click **Delete**. Click **OK** to confirm the deletion or click **Cancel** to cancel the operation. • **Modify**—Click the hyperlinked item in the **Name** column.  Name | Location | Protocol □ service-http | Predefined | TCP □ service-https | Predefined | TCP – Required fields display a light yellow background.  Name escription This field is required – To modify sections within a page (for example, **Devices > Setup**), click the icon in the upper right corner of a section to edit the settings.  Management Interface Settings Speed IP Address 10.5.68.46 – After you configure settings, you must click **OK** or **Save** to store the changes. When you click **OK**, the candidate configuration is updated. To save the changes to the running configuration, you must **Commit** your changes.
4	**Logout**—Click the **Logout** button to log out of the web interface.

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>5</td><td>

- **Tasks**—Click the **Tasks** icon to view the current list of **All** or **Running Tasks**, **Jobs**, and **Log Requests**. Use the **Show** drop-down to filter the list of tasks. The **Task Manager** window displays the list of tasks, along with status, start times, associated messages, and actions.



Task Manager - All Tasks

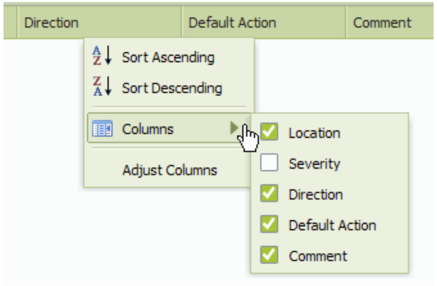
<table>
<tr><th>Type</th><th>Status</th><th>Start Time</th><th>Messages</th><th>Action</th></tr>
<tr><td>Commit</td><td>Completed</td><td>09/09/11 07:57:23</td><td>● In virtual-router vr1: address 10.40.1.1/24 on interface ethernet1/7 is duplicate with address 10.40.1.2/24 on interface ethernet1/8.(Module: routed)
● Commit failed</td><td></td></tr>
<tr><td>Commit</td><td>Completed</td><td>09/09/11 07:56:16</td><td>● In virtual-router vr1: address 10.40.1.1/24 on interface ethernet1/7 is duplicate with address 10.40.1.2/24 on interface ethernet1/8.(Module: routed)
● Commit failed</td><td></td></tr>
<tr><td>Commit</td><td>Completed</td><td>09/09/11 07:52:26</td><td></td><td></td></tr>
<tr><td>Commit</td><td>Completed</td><td>09/09/11 07:49:25</td><td>● Interface ethernet1/7 has no ip pool(Module: dhcpd)
● Configuration committed successfully</td><td></td></tr>
<tr><td>Auto Commit</td><td>Completed</td><td>09/08/11 15:06:15</td><td>● Configuration committed successfully
● Successfully committed last configuration
● L3 Service Configuration is changed. l3svc will be restarted.
● (Module: device)</td><td></td></tr>
</table>

Show All Tasks

- **Language**—Click **Language** to select the desired language from the drop-down in the Language Preference window and then click **OK** to save your change. Unless you specify a language preference, the language on the web interface is the same as the current language of the computer from which you log in. For example, if the computer you use to manage the firewall has a locale of Spanish, the web interface will be in Spanish when you log in to the firewall.
- **Alarms**—Click **Alarms** to view the current list of alarms in the alarms log. To enable Alarms and web alarm notifications, go to **Device > Log Settings > Alarms**. The list displays unacknowledged and acknowledged alarms. To acknowledge alarms, select the check boxes and click **Acknowledge**. This action moves the alarms to the **Acknowledged Alarms** list.

</td></tr>
<tr><td>6</td><td>

The tables allow you to sort data and show or hide columns that you can view on the page. Click a column header to sort on that column and click again to reverse the sort order. To show or hide columns, click the arrow to the right of any column and select or clear the corresponding check box to show or hide the column in the display.



Direction
Default Action
Comment
Sort Ascending
Sort Descending
Columns
Adjust Columns
☑ Location
□ Severity
☑ Direction
☑ Default Action
☑ Comment

</td></tr>
<tr><td>7</td><td>

Use the filter input box to search for terms, names, or keywords for the items on the page. The total number of items on the page are displayed in the left corner of the filter input box. To apply a filter, click →, and to clear a filter, click ☒. The results of the search are displayed and the number of matches appear as a fraction of the total items displayed in the left corner of the filter input box.

</td></tr>
<tr><td>8</td><td>

For information on **Commit**, see“Committing Changes”.

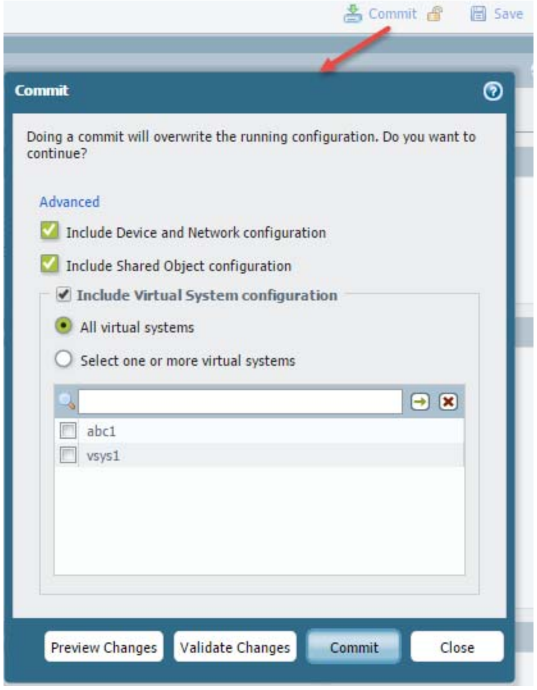
For information on **Locks**, see “Locking Transactions”.

For information on **Search**, see “Searching the Configuration”.

</td></tr>
</table>

Committing Changes

Click **Commit** at the top of the web interface to open the Commit dialog.



Doing a commit will overwrite the running configuration. Do you want to continue?

Advanced

☑ Include Device and Network configuration

☑ Include Shared Object configuration

☑ Include Virtual System configuration

● All virtual systems

○ Select one or more virtual systems

□ abc1

□ vsys1

The following options are available in the Commit dialog. Click the **Advanced** link, if needed, to display the following options:

- **Include Device and Network configuration**—Include the device and network configuration changes in the commit operation.
- **Include Shared Object configuration**—(Only firewalls with multiple virtual systems) Include the shared object configuration changes in the commit operation.
- **Include Policy and Objects**—(Only firewalls that cannot be or are not configured to allow multiple virtual systems) Include the policy and object configuration changes in the commit operation.

*Configuration changes that span multiple configuration areas may require a full commit. For example, if you click **Commit** and select only the **Include Device and Network configuration** option, some items that you changed in the Device tab will not commit. This includes certificates and User-ID™ options, as well as server profiles used for User-ID, such as an LDAP server profile. This can also occur if you perform a partial commit after importing a configuration. To commit these types of changes, do a full commit and select both **Include Device and Network configuration** and **Include Policy and Object configuration** options.*

- **Include Virtual System configuration**—Include all virtual systems or choose **Select one or more virtual systems**.

  For more information about committing changes (see“Defining Operations Settings”).

- **Preview Changes**—Click **Preview Changes** to bring up a two-pane window that shows proposed changes in the candidate configuration compared to the current running configuration. You can choose the number of lines to display, or show all lines. Changes are color-coded based on items that have been added, modified, or deleted. The **Device > Config Audit** feature performs the same function (see “Comparing Configuration Files”).

Because the preview results display in a new window, your browser must allow pop-ups. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-ups.

- **Validate Changes**—Click **Validate Changes** to perform a syntactic validation (whether configuration syntax is correct) and semantic validation (whether the configuration is complete and makes sense) of the firewall configuration before committing the changes. The response will include all of the errors and warnings that a full commit or virtual system commit would, including rule shadowing and application dependency warnings; however, no changes are made to the running configuration. This validation helps you know if a change can be successfully committed before actually committing it, significantly reducing failures at commit time. The **Validate** option is available in Admin Role profiles so that you can control who can validate configurations.

Starting with PAN-OS 7.0 and Panorama™ 7.0, the firewall no longer terminates a commit at the first error. Instead, the firewall collects and displays all errors and then terminates the commit. This allows an administrator to see all the errors immediately upon commit failure and avoids the cycle of multiple commits that return additional errors that also need to be fixed before all changes are finally committed successfully.

Searching the Configuration

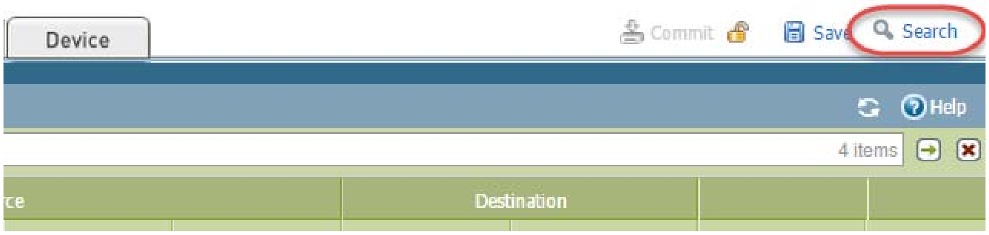
Global Find enables you to search the candidate configuration on a firewall or on Panorama for a particular string, such as an IP address, object name, policy name, threat ID, or application name. The search results are grouped by category and provide links to the configuration location in the web interface,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

The following is a list of Global Find features to help you perform successful searches:

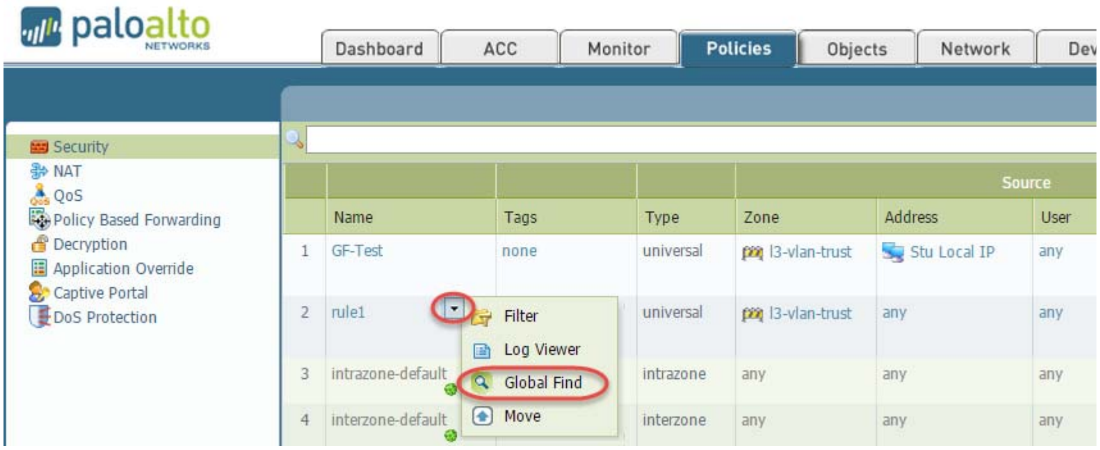
- If you initiate a search on a firewall that has multiple virtual systems enabled or if admin roles are defined, Global Find will only return results for areas of the firewall in which you have permissions. The same applies to Panorama device groups. In this case, you will see search results for any device group to which you have permissions.
- 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 to find it.
- To find an exact phrase, surround the phrase in quotes.
- Global Find searches the candidate configuration.

- To rerun a previous search, click the **Search** icon located on the upper right of the web interface and a list of the last 20 searches will be displayed. Click an item in the list to rerun that search. The search history list is unique to each administrator account.

You can launch Global Find by clicking the **Search** icon located on the upper right of the management web interface or by clicking Global Find from any area of the web interface that supports Global Find. The following screen capture shows the **Search** icon that is visible from all areas of the web interface.



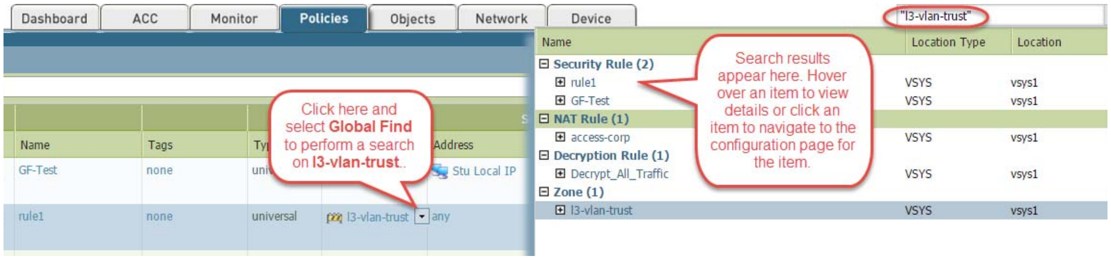
To access the Global Find feature from within a configuration area, click the drop-down next to an item and click **Global Find**. The following screen capture shows the **Global Find** icon that appears when you click the drop-down to the right of a security policy name.



				Source		
	Name	Tags	Type	Zone	Address	User
1	GF-Test	none	universal	l3-vlan-trust	Stu Local IP	any
2	rule1		universal	l3-vlan-trust	any	any
3	intrazone-default		intrazone	any	any	any
4	interzone-default		interzone	any	any	any

The Global Find icon 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**, and **Service**. To perform a search, simply 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, it will search the entire configuration for that zone name and will return results for each location where the zone is referenced. The searched results are grouped by category and you can hover over any item to view details or you can click the item to navigate to the configuration page for that item.

The following screen capture shows the search results for the zone l3-vlan-trust:



Name	Tags	Type		Address
GF-Test	none	uni		Stu Local IP
rule1	none	universal	l3-vlan-trust	any

Name	Location Type	Location
Security Rule (2)		
rule1	VSYS	vsys1
GF-Test	VSYS	vsys1
NAT Rule (1)		
access-corp	VSYS	vsys1
Decryption Rule (1)		
Decrypt_All_Traffic	VSYS	vsys1
Zone (1)		
l3-vlan-trust	VSYS	vsys1

Click here and select **Global Find** to perform a search on **l3-vlan-trust**..

Search results appear here. Hover over an item to view details or click an item to navigate to the configuration page for the item.

Global Find will not search dynamic content (such as logs, address ranges, or individual DHPC addresses) that the firewall allocates to users. 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 user names collected when the User-ID feature is enabled. In this case, a user name or user group that exists in the User-ID database is only searchable if the name or group exists in the configuration, such as defining a user group name in a policy. In general, you can only search on content that the firewall writes to the configuration.

Locking Transactions

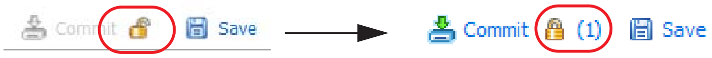
The web interface provides support for multiple administrators by allowing an administrator to lock a current set of transactions, thereby preventing configuration changes or commit operations by another administrator until the lock is removed. The following types of locks are supported:

- **Config Lock**—Blocks other administrators from making changes to the configuration. This type of lock can be set globally or for a virtual system. It can be removed only by the administrator who set the lock or by a superuser on the system.

- **Commit Lock**—Blocks other administrators from committing changes until all of the locks have been released. This type of lock prevents collisions that can occur when two administrators are making changes at the same time and the first administrator finishes and commits changes before the second administrator has finished. The lock is released when the current changes are committed by the administrator who applied the lock; the lock can also be released manually by the administrator who took the lock or by a superuser on the system.

Any administrator can open the Locks window to view the current transactions that are locked, along with a timestamp for each.

To lock a transaction, click the unlocked **Lock** icon 🔓 on the top bar to open the Locks dialog. Click **Take a Lock**, select the scope of the lock from the drop-down, and click **OK**. Add additional locks as needed and then click **Close** to close the Lock dialog. The transaction is locked and the icon on the top bar changes to a locked **Lock** icon that shows the number of locked items in parentheses.



To unlock a transaction, click the locked **Lock** icon 🔒 on the top bar to open the Locks window. Click the ☒ icon for the lock that you want to remove and click **Yes** to confirm. Click **Close** to close the Lock dialog.

You can arrange to automatically acquire a commit lock by selecting the **Automatically acquire commit lock** check box in the Management area of the **Device Setup** page (see "System Setup, Configuration, and License Management").

Supported Browsers

The minimum version of the web browsers supported for accessing the firewall web interface are as follows:

- Internet Explorer 7
- Firefox 3.6
- Safari 5
- Chrome 11

Getting Help Configuring the Firewall

Use the information in this section to obtain help with using the firewall.

Obtaining More Information

To obtain more information about the firewall, refer to the following:

- **General information**—Go to http://www.paloaltonetworks.com.
- **Documentation**—For information on the additional capabilities and for instructions on configuring the features on the firewall, go to https://www.paloaltonetworks.com/documentation.
- **Online help**—Click **Help** in the upper-right corner of the web interface to access the online help system.
- **Knowledge Base**—For access to the knowledge base, a collaborative area for customer and partner interaction, discussion forums, and videos, go to https://live.paloaltonetworks.com.

Technical Support

For technical support, for information on support programs, or to manage your account or devices, go to https://www.paloaltonetworks.com/support/tabs/overview.html.

Chapter 3

Device Management

Use the following sections for field reference on basic system configuration and maintenance tasks on the firewall:

- "System Setup, Configuration, and License Management"
- "Defining VM Information Sources"
- "Installing the Software"
- "Updating Threat and Application Definitions"
- "Administrator Roles, Profiles, and Accounts"
- "Setting Up Authentication Profiles"
- "Creating a Local User Database"
- "Adding Local User Groups"
- "Configuring RADIUS Server Settings"
- "Configuring TACACS+ Server Settings"
- "Configuring LDAP Server Settings"
- "Configuring Kerberos Server Settings"
- "Setting Up an Authentication Sequence"
- "Creating a Certificate Profile"
- "Scheduling Log Exports"
- "Defining Logging Destinations"
- "Configuring Netflow Settings"
- "Using Certificates"
- "Encrypting Private Keys and Passwords on the Firewall"
- "Enabling HA on the Firewall"
- "Defining Virtual Systems"
- "Defining Custom Response Pages"
- "Viewing Support Information"

System Setup, Configuration, and License Management

The following sections describe how to define network settings for management access, defining service routes and services, and how to manage configuration options such as global session timeouts, content identification, WildFire™ malware analysis and reporting:

- "Defining Management Settings"
- "Defining Operations Settings"
- "Defining Hardware Security Modules"
- "Enabling SNMP Monitoring"
- "Defining Services Settings"
- "Defining a DNS Server Profile"
- "Defining Content-ID Settings"
- "Configuring WildFire Settings"
- "Defining Session Settings"
- "Comparing Configuration Files"
- "Installing a License"

Defining Management Settings

▶ ***Device* > *Setup* > *Management***

▶ ***Panorama* > *Setup* > *Management***

On a firewall, use the **Device** > **Setup** > **Management** tab to configure management settings. On Panorama™, use the **Device** > **Setup** > **Management** tab to configure firewalls that you manage with Panorama templates. Use the **Panorama** > **Setup** > **Management** tab to configure settings for Panorama.

For firewall management, optionally you can use the IP address of a loopback interface instead of the management port (see "Configure a Loopback Interface").

Configure the following management settings. These apply to both the firewall and Panorama, except where otherwise noted.

- "General Settings"
- "Authentication Settings"
- "Panorama Settings: Device > Setup > Management" (settings configured on the firewall to connect to Panorama)
- "Panorama Settings: Panorama > Setup > Management" (settings configured on Panorama to connect to the firewalls)
- "Management Interface Settings"

- “Eth1 Interface Settings” (Panorama only)
- “Eth2 Interface Settings” (Panorama only)
- “Logging and Reporting Settings”
- “Minimum Password Complexity”

Table 1. Management Settings

Item	Description
General Settings	
Hostname	Enter a host name (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Domain	Enter the Fully Qualified Domain Name (FQDN) of the firewall (up to 31 characters).
Login Banner	Enter custom text that will be displayed on the firewall login page. The text is displayed below the **Name** and **Password** fields.
SSL/TLS Service Profile	Assign an existing SSL/TLS Service profile or create a new one to specify a certificate and the allowed protocols for securing inbound traffic on the management interface of the device. For details, see “Managing SSL/TLS Service Profiles”. If you select **none**, the device uses the preconfigured, self-signed certificate. **Note:** *Best practice is not to use the default certificate. For better security, it is recommended that you assign a SSL/TLS Service profile associated with a certificate that a trusted certificate authority (CA) has signed.*
Time Zone	Select the time zone of the firewall.
Locale	Select a language for PDF reports from the drop-down. See “Managing PDF Summary Reports”. If you have a specific language preference set for the web interface, PDF reports will still use the language specified in this locale setting. See language preference in “Using the Palo Alto Networks Firewall Web Interface”.
Time	Set the date and time on the firewall: • Enter the current date (in YYYY/MM/DD format), or select the date from the drop-down. • Enter the current time in 24-hour format (HH:MM:SS). **Note:** *You can also define an NTP server from **Device > Setup > Services**.*
Serial Number (Panorama virtual machines only)	Enter the serial number for Panorama. Find the serial number in the order fulfillment email that was sent to you.
Geo Location	Enter the latitude (-90.0 to 90.0) and longitude (-180.0 to 180.0) of the firewall.
Automatically acquire commit lock	Select the check box to automatically apply a commit lock when you change the candidate configuration. For more information, see “Locking Transactions”.
Certificate Expiration Check	Instruct the firewall to create warning messages when on-box certificates near their expiration dates.

Table 1. Management Settings (Continued)

Item	Description
Multi Virtual System Capability	Enables the use of multiple virtual systems on firewalls that support this feature (see “Defining Virtual Systems”).
URL Filtering Database (Panorama only)	Select a URL Filtering vendor for use with Panorama: **brightcloud** or **paloaltonetworks** (PAN-DB).
Use Hypervisor Assigned MAC Addresses (VM-Series firewalls only)	Select the check box 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 must not 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 the EUI-64 format is used.
Authentication Settings	
Authentication Profile	Select the authentication profile (or sequence) to use for authenticating administrators who have external accounts (accounts that are not defined on the device). Only authentication profiles that have a type set to RADIUS and that reference a RADIUS server profile are available for this setting. When external administrators log in, the device requests authentication information (including the administrator role) from the RADIUS server. To enable authentication for external administrators, you must also install the Palo Alto Networks® RADIUS dictionary file on the RADIUS server. This file defines authentication attributes needed for communication between the device and the RADIUS server. Refer to the RADIUS server software documentation for instructions on where to install the file. If you select **None**, the device won’t authenticate external administrators; they cannot log in. For details, see “Setting Up Authentication Profiles” and “Configuring RADIUS Server Settings”. **Note:** *If an administrator is local, the device uses the authentication profile associated with the administrator account for authentication (see “Creating Administrative Accounts”).*
Certificate Profile	Select the certificate profile to use for administrator access to the firewall. For instructions on configuring certificate profiles, see “Creating a Certificate Profile”.
Idle Timeout	Enter the timeout interval in minutes (range is 0-1440, default is 0). A value of 0 means that the management, web interface, or CLI session does not time out.
Failed Attempts	Enter the number of failed login attempts (range is 0-10) that the device allows for the web interface and CLI before locking out the user account. A value of 0 (default) means there is no limit. **CAUTION:** *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.*

Table 1. Management Settings (Continued)

Item	Description
Lockout Time	Enter the number of minutes (range is 0-60) for which PAN-OS locks out a user from access to the web interface and CLI after reaching the **Failed Attempts** limit. A value of 0 (default) means the lockout applies until an administrator manually unlocks the user account. **CAUTION:** *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.*
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: see "Panorama Settings: Panorama > Setup > Management". **Note:** *The firewall uses an SSL connection with AES-256 encryption to register with Panorama. Panorama and the firewall authenticate each other using 2,048-bit certificates and use the SSL connection for configuration management and log collection.*	
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 1-240, default is 240).
Send Timeout for Connection to Panorama	Enter the timeout in seconds for sending TCP messages to Panorama (range is 1-240, 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 1-64, default is 25).
Disable/Enable Panorama Policy and Objects	This button appears when you edit the **Panorama Settings** on a firewall (not in a template on Panorama). Clicking **Disable Panorama Policy and Objects** disables 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 the button, select the **Import Panorama Policy and Objects before disabling** check box. After you perform a commit, the 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**.

Table 1. Management Settings (Continued)

Item	Description
Disable/Enable Device and Network Template	This button appears when you edit the **Panorama Settings** on a firewall (not in a template on Panorama). Clicking **Disable Device and Network Template** disables the propagation of template information (device and network configurations) to 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 click the button, select the **Import Device and Network Templates before disabling** check box. 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". **Note:** *The firewall uses an SSL connection with AES-256 encryption to register with Panorama. Panorama and the firewall authenticate each other using 2,048-bit certificates and use the SSL connection for configuration management and log collection.*	
Receive Timeout for Connection to Device	Enter the timeout in seconds for receiving TCP messages from all managed firewalls (range is 1-240, default is 240).
Send Timeout for Connection to Device	Enter the timeout in seconds for sending TCP messages to all managed firewalls (range is 1-240, 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 1-64, default is 25).
Share Unused Address and Service Objects with Devices	Select this check box to share all Panorama shared objects and device-group-specific objects with managed firewalls. This setting is enabled by default. If you clear the check box, PAN-OS checks Panorama policies for references to address, address group, service, and service group objects, and does not share any unreferenced objects. This option reduces the total object count by ensuring that PAN-OS sends only necessary objects to managed firewalls.

Table 1. Management Settings (Continued)

Item	Description
Objects defined in ancestors will take higher precedence	Select the check box to specify that when device groups at different levels in the hierarchy have objects of the same type and name but different values, the object values in ancestor groups take precedence over those in descendant groups. This means that when you perform a device group commit, the ancestor values replace any override values. By default, this system-wide setting is disabled and objects that you override in a descendant group take precedence in that group over objects inherited from ancestor groups.
Management Interface Settings This interface applies to the firewall, Panorama M-Series appliance, or Panorama virtual appliance. By default, the M-Series appliance uses the management (MGT) interface for configuration, log collection, and collector group communication. However, if you configure Eth1 or Eth2 for log collection or collector group communication, best practice is to define a separate subnet for the MGT interface that is more private than the Eth1 or Eth2 subnets. Define the subnet in the **Netmask** (for IPv4) or **IPv6 Address/Prefix Length** (for IPv6) field. The Panorama virtual appliance does not support separate interfaces. **Note:** *To complete the configuration of the management 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 only access the device via the console port for future configuration changes. It is recommended that you always commit a complete configuration.*	
IP Address (IPv4)	If your network uses IPv4, assign an IPv4 address to the management interface. Alternatively, you can assign the IP address of a loopback interface for device management. By default, the IP address you enter is the source address for log forwarding.
Netmask (IPv4)	If you assigned an IPv4 address to the management interface, you must also enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to the management interface, you must also assign an IPv4 address to the default gateway (the gateway must be on the same subnet as the management interface).
IPv6 Address/Prefix Length	If your network uses IPv6, assign an IPv6 address to the management 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 management interface, you must also assign an IPv6 address to the default gateway (the gateway must be on the same subnet as the management interface).
Speed	Configure a data rate and duplex option for the management interface. The choices include 10Mbps, 100Mbps, and 1Gbps at full or half duplex. Use the default auto-negotiate setting to have the device (Panorama or the firewall) determine the interface speed. **CAUTION:** *This setting must match the port settings on the neighboring network equipment.*
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576-1500, default is 1500).
Services	Select the services you want enabled on the specified management interface address: HTTP, HTTP OCSP, HTTPS, Telnet, SSH (Secure Shell), Ping, SNMP, User-ID™, User-ID Syslog Listener-SSL, User-ID Syslog Listener-UDP.

Table 1. Management Settings (Continued)

Item	Description
Permitted IP Addresses	Enter the list of IP addresses from which firewall management is allowed. When using this option for the Panorama M-Series appliance, add the IP address of each managed firewall. Otherwise the firewall cannot connect and forward logs to Panorama or receive configuration updates.
Eth1 Interface Settings This interface only applies to the Panorama M-Series appliance. By default, the M-Series appliance uses the management interface for configuration, log collection, and collector group communication. However, if you enable Eth1, you can configure it for log collection or collector group communication when you define managed collectors (**Panorama > Managed Collectors**). **Note:** *You cannot commit the Eth1 configuration unless you specify the IP address, the netmask (for IPv4) or prefix length (for IPv6), and the default gateway.*	
Eth1	Select this check box to enable the Eth1 interface.
IP Address (IPv4)	If your network uses IPv4, assign an IPv4 address to the Eth1 interface.
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 Eth1 interface).
IPv6 Address/Prefix Length	If your network uses IPv6, you must also assign an IPv6 address to the Eth1 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 Eth1 interface).
Speed	Configure a data rate and duplex option for the Eth1 interface. The choices include 10Mbps, 100Mbps, and 1Gbps at full or half duplex. Use the default auto-negotiate setting to have Panorama determine the interface speed. **CAUTION:** *This setting must match the port settings on the neighboring network equipment.*
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576-1500, default is 1500).
Services	Select **Ping** if you want to enable that service on the Eth1 interface.
Permitted IP Addresses	Enter the list of IP addresses from which Eth1 management is allowed.
Eth2 Interface Settings This interface only applies to the Panorama M-Series appliance. By default, the M-Series appliance uses the management interface for configuration, log collection, and collector group communication. However, if you enable Eth2, you can configure it for log collection and/or collector group communication when you define managed collectors (**Panorama > Managed Collectors**). **Note:** *You cannot commit the Eth2 configuration unless you specify the IP address, the netmask (for IPv4) or prefix length (for IPv6), and the default gateway.*	
Eth2	Select this check box to enable the Eth2 interface.
IP Address (IPv4)	If your network uses IPv4, assign an IPv4 address to the Eth2 interface.

Table 1. **Management Settings (Continued)**

Item	Description
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 Eth2 port).
IPv6 Address/Prefix Length	If your network uses IPv6, assign an IPv6 address to the Eth2 interface. To indicate the netmask, enter an IPv6 prefix length (for example, 2001:400:f00::1/64).
Default IPv6 Gateway	If you specified 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 Eth2 interface).
Speed	Configure a data rate and duplex option for the Eth2 interface. The choices include 10Mbps, 100Mbps, and 1Gbps at full or half duplex. Use the default auto-negotiate setting to have Panorama determine the interface speed. **CAUTION:** *This setting must match the port settings on the neighboring network equipment.*
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576-1500, default is 1500).
Services	Select **Ping** if you want to enable that service on the Eth2 interface.
Permitted IP Addresses	Enter the list of IP addresses from which Eth2 management is allowed.

Table 1. Management Settings (Continued)

Item	Description
Logging and Reporting Settings Use this section to modify: • Expiration periods and storage quotas for the logs and reports that the following devices generate. The settings are synchronized across high availability pairs. – Logs that a firewall generates (**Device > Setup > Management**). The settings apply to all the virtual systems on the firewall. – Logs that a Panorama management server and its managed collectors generate (**Panorama > Setup > Management**). To configure the settings for logs that a managed collector receives from firewalls, see "Defining Log Collector Groups". • Attributes for calculating and exporting user activity reports. • Predefined reports created on the firewall/Panorama.	
Log Storage subtab (The **Log Card Storage** and **Management Card Storage** tabs are only applicable to the PA-7000 Series firewalls)	For each log type and log summary type, specify: • The **Quota** allocated on the hard disk for log storage, as a percentage. When you change a **Quota** value, the associated disk allocation changes automatically. If the total of all the values exceeds 100%, a message appears on the page in red, and an error message appears when you try to save the settings. If this happens, adjust the percentages so the total is within the 100% limit. • The **Max Days**, which is the log expiration period (range is 1-2,000). The device automatically deletes logs that exceed the specified period. By default, no expiration period is set, which means logs never expire. The device evaluates logs as it creates them and deletes logs that exceed the expiration period or quota size. **CAUTION:** *Weekly summary logs can age beyond the threshold before the next deletion if they reach the expiration threshold between times when the device deletes logs. When a log quota reaches the maximum size, the device starts overwriting the oldest log entries with the new log entries. If you reduce a log quota size, the device removes the oldest logs when you commit the changes. In a high availability (HA) active/passive configuration, the passive peer does not receive logs and, therefore, does not delete them unless failover occurs and it becomes active.* Click **Restore Defaults** to revert to the default values. Click **OK** to save changes. The PA-7000 Series firewalls store logs in the Log Processing Card (LPC) and Switch Management Card (SMC), and divide log quotas into these two areas. The **Log Storage** tab has quota settings for data-type traffic stored on the LPC (for example, traffic and threat logs). The **Management Card Storage** tab has quota settings for management-type traffic stored on the SMC (for example, the Config logs, System logs, and Alarms logs).

Table 1. Management Settings (Continued)

Item	Description
Log Export and Reporting subtab	**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 from the **Export to CSV** icon in the traffic logs view (range is 1-1048576, default is 65535). **Max Rows in User Activity Report**—Enter the maximum number of rows that is supported for the detailed user activity reports (range is 1-1048576, default is 5000). **Average Browse Time (sec)**—Configure this variable to adjust how the browse time is calculated in seconds for the “User Activity Report” (range is 0-300 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 admin 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. **Page Load Threshold (sec)**—This option allows you to adjust the assumed time in seconds that it takes for page elements to load on the page (range is 0-60, 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 “User Activity Report”. **Syslog HOSTNAME Format**—Select whether to use the FQDN, hostname, IP address (v4 or V6) in the syslog message header; this header identifies the firewall/Panorama from which the message originated. **Stop Traffic when LogDb full**—(Firewall only) Select the check box if you want traffic through the firewall to stop when the log database is full (default is off). **Report Expiration Period**—Set the expiration period in days for reports (range is 1-2,000). By default, no expiration period is set, which means reports never expire. The device deletes expired reports nightly at 2 a.m. according to the time on the device.

Table 1. Management Settings (Continued)

Item	Description
	Enable Log on High DP Load—(Firewall only) Select this check box if you would like a system log entry generated when the packet processing load on the firewall is at 100% 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 the probable cause. Disabled by default.
(Only on Panorama)	**Buffered Log Forwarding from Device**—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 log entries are forwarded to Panorama; the disk space available for buffering depends on the log storage quota for the platform 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. Enabled by default. **Get Only New Logs on Convert to Primary**—This option is only applicable when Panorama writes logs to a Network File Share (NFS). With NFS logging, only the *primary* Panorama is mounted to the NFS. Therefore, the firewalls send logs to the *active primary* Panorama only. This option allows an administrator to configure the managed firewalls to only send newly generated logs to Panorama when an HA failover occurs and the secondary Panorama resumes logging to the NFS (after it is promoted as primary). This behavior is typically enabled to prevent the 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**—Allows you to configure only the active primary Panorama to save logs to the local disk. This option is valid for a Panorama virtual machine with a virtual disk and to the M-Series appliance in Panorama mode.
	Pre-Defined Reports—Pre-defined reports for application, traffic, threat, and URL Filtering are available on the firewall and on Panorama. By default, these pre-defined reports are enabled. 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 you can disable the reports that are not relevant to you; to disable a report, clear the check box for the report. Use the **Select All** or **Deselect All** options to entirely enable or disable the generation of pre-defined reports. **Note:** *Before disabling a report make sure that the report is not included in a Group Report or a PDF Report. If a pre-defined report is part of a set of reports and it is disabled, the entire set of reports will have no data.*

Table 1. Management Settings (Continued)

Item	Description
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 "Defining Password Profiles" and see "Defining Administrator Roles" for information on valid characters that can be used for accounts. ***Note:*** *The maximum password length that can be entered is 31 characters. When setting requirements, make sure you do not create a combination that will not be accepted. Example, you would not be able to set a requirement of 10 uppercase, 10 lower case, 10 numbers, and 10 special characters since that would exceed the maximum length of 31.* **Note:** *If you have High Availability (HA) configured, always use the primary device when configuring password complexity options and commit soon after making changes.*
Minimum Length	Require minimum length from 1-15 characters.
Minimum Uppercase Letters	Require a minimum number of uppercase letters from 0-15 characters.
Minimum Lowercase Letters	Require a minimum number of lowercase letters from 0-15 characters.
Minimum Numeric Letters	Require a minimum number of numeric letters from 0-15 numbers.
Minimum Special Characters	Require a minimum number of special characters (non-alphanumeric) from 0-15 characters.
Block Repeated Characters	Specify the number of sequential duplicate characters permitted in a password. The range is (2-15). 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 check box 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 check box to prompt the administrators to change their passwords the first time they log in to the device.
Prevent Password Reuse Limit	Require that a previous password is not reused based on the specified count. Example, if the value is set to 4, you could not reuse the any of your last 4 passwords (range 0-50).
Block Password Change Period (days)	User cannot change their passwords until the specified number of days has been reached (range 0-365 days).

Table 1. Management Settings (Continued)

Item	Description
Required Password Change Period (days)	Require that administrators change their password on a regular basis specified a by the number of days set, ranging from 0-365 days. 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 0-30 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 0-30 days).
Allowed expired admin login (count)	Allow the administrator to log in the specified number of times after the 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 0-3 logins).
Post Expiration Grace Period (days)	Allow the administrator to log in the specified number of days after the account has expired (range 0-30 days).

Defining Operations Settings

▶ *Device > Setup > Operations*

▶ *Panorama > Setup > Operations*

When you change a configuration setting and click **OK**, the current candidate configuration is updated, not the active configuration. Clicking **Commit** at the top of the page applies the candidate configuration to the active configuration, which activates all configuration changes since the last commit.

This method allows you to review the configuration before activating it. Activating multiple changes simultaneously helps avoid invalid configuration states that can occur when changes are applied in real-time.

You can save and roll back (restore) the candidate configuration as often as needed and also load, validate, import, and export configurations. Pressing **Save** creates a copy of the current candidate configuration, whereas choosing **Commit** updates the active configuration with the contents of the candidate configuration.

*It is a good idea to periodically save the configuration settings you have entered by clicking the **Save** link in the upper-right corner of the screen.*

You can use Secure Copy (SCP) commands from the CLI to export configuration files, logs, reports, and other files from a device to an SCP server and import the files to another device. However, because the log database is too large for an export or import to be practical on the following platforms, they do not support exporting or importing the entire log database: PA-7000 Series firewalls (all PAN-OS releases), Panorama virtual appliance running Panorama 6.0 or later releases, and Panorama M-Series appliances (all Panorama releases).

To manage configurations, select the appropriate configuration management functions, as described in the following table.

Table 2. Configuration Management Functions

Function	Description
Configuration Management	
Revert to last saved config	Restores the last saved candidate configuration from the local drive. The current candidate configuration is overwritten. An error occurs if the candidate configuration has not been saved.
Revert to running config	Restores the last running configuration. The current running configuration is overridden.
Save named configuration snapshot	Saves the candidate configuration to a file. Enter a file name or select an existing file to be overwritten. Note that the current active configuration file (*running-config.xml*) cannot be overwritten.
Save candidate config	Saves the candidate configuration in flash memory (same as clicking **Save** at the top of the page).
Load named configuration snapshot	Loads a candidate configuration from the active configuration (*running-config.xml*) or from a previously imported or saved configuration. Select the configuration file to be loaded. The current candidate configuration is overwritten.
Load configuration version	Loads a specified version of the configuration.
Export named configuration snapshot	Exports the active configuration (*running-config.xml*) or a previously saved or imported configuration. Select the configuration file to be exported. You can open the file and/or save it in any network location.
Export configuration version	Exports a specified version of the configuration.
Export Panorama and devices config bundle (Panorama only)	Manually generates and exports the latest versions of the running configuration backup of Panorama and of each managed firewall. To automate the process of creating and exporting the configuration bundle daily to an SCP or FTP server, see “Scheduling Configuration Exports”.
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. For related information, see “Import Device Configuration to 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. **WARNING:** *These options are available only for firewalls running PAN-OS 6.0.4 and later releases.*

Table 2. Configuration Management Functions (Continued)

Function	Description
Export device state (firewall only)	Exports the configuration and dynamic information from a firewall that is configured as a GlobalProtect™ Portal with the Large Scale VPN (LSVPN) feature enabled. If the Portal experiences a failure, the export file can be imported to restore the Portal's configuration and dynamic information. The export contains a list of all satellite devices managed by the Portal, the running configuration at the time of the export, and all certificate information (Root CA, Server, and Satellite certificates). **Important:** You must manually run the device 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 since satellite certificates may change often. To create the device state file from the CLI, from configuration mode run `save device state`. The file will be named device_state_cfg.tgz and is stored in /opt/pancfg/mgmt/device-state. The operational command to export the device state file is `scp export device-state` (you can also use `tftp export device-state`). For information on using the XML API, refer to the "PAN-OS XML-Based Rest API Usage Guide" at http://www.paloaltonetworks.com/documentation.
Import named config snapshot	Imports a configuration file from any network location. Click **Browse** and select the configuration file to be imported.
Import device state (firewall only)	Imports the firewall state information that was exported using the Export device state option. This includes the current running config, Panorama templates, and shared policies. If the device is a GlobalProtect Portal, the export includes the Certificate Authority (CA) information and the list of satellite devices and their authentication information.

Table 2. Configuration Management Functions (Continued)

Function	Description
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 “Defining Device Groups”). **WARNING:** *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 only lists 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. • **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**—This check box is selected by default, which means Panorama imports objects that belong to Shared in the firewall to Shared in Panorama. If you clear the check box, 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 the check box. – 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 the check box. • **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. **WARNING:** *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 else the commit will fail.*

Table 2. Configuration Management Functions (Continued)

Function	Description
Device Operations	
Reboot	To restart the firewall or Panorama, click **Reboot Device**. The device logs you out, reloads the software (PAN-OS or Panorama) and 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 “Defining Operations Settings”). **Note:** *If the web interface is not available, use the CLI command* `request restart system`.
Shutdown	To perform a graceful shutdown of the firewall/Panorama, click **Shutdown Device** or **Shutdown Panorama** and then click **Yes** on the confirmation prompt. Any configuration changes that have not been 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 device will powered off. You need to unplug the power source and plug it back in before you can power on the device. ***Note:*** *If the web interface is not available, use the CLI command* `request shutdown system`.
Restart Data Plane	To restart the data functions of the firewall without rebooting, click **Restart Dataplane**. *This option is not available on the PA-200 firewall and on Panorama.* **Note:** *If the web interface is not available, use the CLI command* `request restart dataplane`.

Table 2. Configuration Management Functions (Continued)

Function	Description
Miscellaneous	
Custom Logos	Use this option to customize any of the following: • Login screen background image • Main UI (User Interface) header image • PDF report title page image. Refer to "Managing PDF Summary Reports". • PDF report footer image Click ⤓ to upload an image file, 🔍 to preview, or ⊟ to remove a previously-uploaded image. Note the following: • Supported file types are png, gif, and jpg. *Image files that contain an alpha channel are not supported and when used in PDF reports, the reports will not be generated properly. You may need to contact the illustrator who created the image to remove alpha channels in the image or make sure the graphics software you are using does not save files with the alpha channel feature.* • To return to the default logo, remove your entry and commit. • The maximum image size for any logo image is 128 KB. • For the login screen and main user interface options, when you click 🔍, the image is shown as it will be displayed. If necessary, the image is cropped to fit. For the PDF reports, the images are auto-resized to fit without cropping. In all cases, the preview shows the recommended image dimensions. For information on generating PDF reports, see "Managing PDF Summary Reports".
SNMP Setup	Specify SNMP parameters. See "Enabling SNMP Monitoring".
Statistics Service Setup	The **Statistics Service** feature allows the firewall to send anonymous application, threat, and crash information to the Palo Alto Networks research team. The information collected enables the research team to continually improve the effectiveness of Palo Alto Networks products based on real-world information. This service is disabled by default and once enabled, information will be uploaded every 4 hours. You can allow the firewall to send any of the following types of information: • Application and Threat Reports • Unknown Application Reports • URL Reports • Device traces for crashes To view a sample of the content for a statistical report to be sent, click the report icon 📄. The **Report Sample** tab opens to display the report code. To view a report, click the check box next to the desired report, then click the **Report Sample** tab.

Defining Hardware Security Modules

▶ *Device > Setup > HSM*

The **HSM** tab allows you to view status and configure a Hardware Security Module (HSM). The following status settings are displayed in the Hardware Security Module Provider section.

Table 3. HSM Module Provider Status settings

Field	Description
Provider Configured	Specifies one of the following: • **None** – No HSM is configured for the firewall. • **SafeNet Luna SA** – A SafeNet Luna SA HSM is configured on the firewall. • **Thales Nshield Connect** – A Thales Nshield Connect HSM is configured on the firewall.
High Availability	HSM high availability is configured if checked. SafeNet Luna SA only.
High Availability Group Name.	The group name configured on the firewall for HSM high availability. SafeNet Luna SA only.
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**.
Master Key Secured by HSM	If checked, the master key is secured on the HSM.
Status	See “SafeNet Luna SA Hardware Security Module Status settings” or “Thales Nshield Connect Hardware Security Module Status settings” as required.

To configure a Hardware Security Module (HSM) on the firewall, click the Edit icon in the Hardware Security Module Provider section and configure the following settings.

Table 4. HSM Configuration Settings

Field	Description
Provider Configured	Specify one of the following: • **None** – No HSM is configured for the firewall. No other configuration required. • **SafeNet Luna SA** – A SafeNet Luna SA HSM is configured on the firewall. • **Thales Nshield Connect** – A Thales Nshield Connect HSM is configured on the firewall.
Module Name	Specify a module name for the HSM. This can be any ASCII string up to 31 characters long. Create multiple module names if you are configuring a high availability HSM configuration.
Server Address	Specify an IPv4 address for any HSM modules you are configuring.
High Availability SafeNet Luna SA only	Select this check box if you are configuring the HSM modules in a high availability configuration. The module name and server address of each HSM module must be configured.

Table 4. HSM Configuration Settings (Continued)

Field	Description
Auto Recovery Retry SafeNet Luna SA 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 high availability configuration. Range 0 -500.
High Availability Group Name. SafeNet Luna SA only	Specify a group name to be used for the HSM high availability group. This name is used internally by the firewall. It can be any ASCII string up to 31 characters long.
Remote Filesystem Address Thales Nshield Connect Only	Configure the IPv4 address of the remote file system used in the Thales Nshield Connect HSM configuration.

Select Setup Hardware Security Module and configure the following settings to authenticate the firewall to the HSM.

Table 5. Setup Hardware Security Module settings

Field	Description
Server Name	Select an HSM server name from the drop down box.
Administrator Password	Enter the administrator password of the HSM to authenticate the firewall to the HSM.

The Hardware Security Module Status section provides the following information about HSMs that have been successfully authenticated. The display is different depending on the HSM provider configured.

Table 6. SafeNet Luna SA Hardware Security Module Status settings

Field	Description
Serial Number	The serial number of the HSM partition is displayed if the HSM partition was successfully authenticated.
Partition	The partition name on the HSM that was assigned on the firewall.
Module State	The current operating state of the HSM. This setting will have the value **Authenticated** if the HSM is displayed in this table.

Table 7. Thales Nshield Connect Hardware Security Module Status settings

Field	Description
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. • **Authenticated** • **Not Authenticated**

Enabling SNMP Monitoring

▶ *Device > Setup > Operations*

Simple Network Management Protocol (SNMP) is a standard protocol for monitoring the devices on your network. Use the **Operations** page to configure the device 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 Palo Alto Networks devices, see Supported MIBs.

To configure the server profile that enables the firewall to communicate with the SNMP trap destinations on your network (see “Configuring SNMP Trap Destinations”). The SNMP MIBs define all SNMP traps that the devices generate. 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 the **SNMP Setup** link and specify the following settings to allow SNMP GET requests from your SNMP manager:

Table 8. SNMP Setup

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 device 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 check box is selected by default, which means the device uses a unique OID for each SNMP trap based on the event type. If you clear this check box, 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 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. As a best practice, 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).

Table 8. SNMP Setup (Continued)

Field	Description
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 device. 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. **Note:** *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 devices forward traps and SNMP managers get device 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 device 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 device uses the password to authenticate to the SNMP manager when forwarding traps and responding to statistics requests. The device 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 device uses the password and Advanced Encryption Standard (AES-128) to encrypt SNMP traps and responses to statistics requests. The password must be 8-256 characters and all characters are allowed.

Defining Services Settings

▶ *Device > Setup > Services*

On a firewall where multiple virtual systems are enabled, the **Services** tab is divided into **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, there are not two tabs, but just a **Services** menu.)

Use the **Global** tab 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.

- In the **Services** section, click the Edit icon to define the destination IP addresses of Domain Name System (DNS) servers, the Update Server, and Proxy Server. Use the dedicated **NTP** tab to configure Network Time Protocol settings. See Table 9 for field descriptions of the options available in the **Services** section.
- In the **Service Features** section, 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, navigate to **Device > Setup > Management** and edit the Management Interface Settings section.
  - 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 Updates.) 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 10, 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. The **Destination** 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 10 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.

Table 9 describes the global services.

Table 9. Services Settings

Function	Description
Services	
DNS	Choose the type of DNS service: **Server** or **DNS Proxy Object**. This setting is used for all DNS queries initiated by the firewall in support of FQDN address objects, logging, and device management. Options include: • Primary and secondary DNS servers to provide domain name resolution. • A DNS proxy that has been configured on the firewall is an alternative to configuring DNS servers.

Table 9. Services Settings (Continued)

Function	Description
Primary DNS Server	Enter the IP address of the primary DNS server. The server is used for DNS queries from the firewall, for example, to find the update server, to resolve DNS entries in logs, or for FDQN-based address objects.
Secondary DNS Server	Enter the IP address of a secondary DNS server to use if the primary server is unavailable (optional).
Update Server	This setting represents the IP address or host name of the server used to download updates from Palo Alto Networks. The current value is **updates.paloaltonetworks.com**. Do not change the server name unless instructed by technical support.
Verify Update Server Identity	If this option is enabled, 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 option adds an additional level of security for the communication between the firewall/Panorama server and the update server.
Proxy Server section	
Server	If the device needs to use a proxy server to reach Palo Alto Networks update services, enter the IP address or host name of the server.
Port	Enter the port for the proxy server.
User	Enter the user name to access the server.
Password/Confirm Password	Enter and confirm the password for the user to access the proxy server.
NTP	
NTP Server Address	Enter the IP address or hostname of an NTP server that you want to use to synchronize the firewall's clock. Optionally enter the IP address or hostname of a second NTP server to synchronize the firewall's clock with if the primary server becomes unavailable.
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 the NTP server's time updates. If you select Symmetric Key, continue by entering the following fields: –**Key ID—**Enter the Key ID (1- 65534). –**Algorithm—**Select the Algorithm to use in NTP authentication (MD5 or SHA1). –**Authentication Key/Confirm Authentication Key—**Enter and confirm the authentication algorithm's authentication key. • **Autokey—**Select this option for the firewall to use autokey (public key cryptography) to authenticate the NTP server's time updates.

Table 10. Service Route Configuration Settings

Service	Global		Virtual System	
	IPv4	IPv6	IPv4	IPv6
CRL Status—Certificate revocation list (CRL) server.	✓	✓	—	—
DNS—Domain Name System server. * For virtual systems, DNS is done in the DNS Server Profile.	✓	✓	✓ *	✓ *
Email—Email server.	✓	✓	✓	✓
HSM—Hardware security module server.	✓	—	—	—
Kerberos—Kerberos authentication server.	✓	—	✓	—
LDAP—Lightweight Directory Access Protocol server.	✓	✓	✓	✓
MDM—Mobile Device Management server.	✓	✓	—	—
Netflow—Netflow server for collecting network traffic statistics.	✓	✓	✓	✓
NTP—Network Time Protocol server.	✓	✓	—	—
Palo Alto Updates—Updates from Palo Alto Networks.	✓	—	—	—
Panorama—Palo Alto Networks Panorama server.	✓	✓	—	—
Proxy—Server that is acting as Proxy to the firewall.	✓	✓	—	—
RADIUS—Remote Authentication Dial-in User Service server.	✓	✓	✓	✓
SNMP Trap—Simple Network Management Protocol trap server.	✓	—	✓	—
Syslog—Server for system message logging.	✓	✓	✓	✓
Tacplus—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.	✓	✓	—	—
VM Monitor—Virtual Machine Monitor server.	✓	✓	✓	✓
WildFire Private—Private Palo Alto Networks WildFire server.	✓	—	—	—
WildFire Public—Public Palo Alto Networks WildFire server.	✓	—	—	—

When customizing a **Global** service route, on either the **IPv4** or **IPv6** tab, select from the list of available services, click **Set Selected Service Routes**, and select the **Source Interface** and **Source Address** from the drop-down. A Source Interface that is set to **Any** allows you to select a Source Address from any of the interfaces available. The Source Address displays the IPv4 or IPv6 address assigned to the selected interface; the selected IP address will be the source for the service traffic. You do not have to define a destination address because the destination is configured when configuring each service. For example, when you define your DNS servers from the **Device > Setup > Services** tab, that will set the destination for DNS queries.

When configuring service routes for a **Virtual System**, the **Inherit Global Service Route Configuration** option means that all services for the virtual system will inherit the global service route settings. Or you can choose **Customize**, select IPv4 or IPv6, select a service, and click **Set Selected Service Routes**. The **Source Interface** has the following three choices:

- **Inherit Global Setting—**The selected services will 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—For the services being configured, the server's responses will be sent to the selected interface because that was the source interface.

For **Source Address**, select an address from the drop-down. For the services selected, the server's responses will be sent to this source address.

Destination Service Route

▶ *Device > Setup > Services > Global*

Returning to 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.

A destination service route can be used to add a customized redirection of a service that is not supported on the **Customize** list of services (Table 10). 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.

Table 11 defines the fields for the **Destination** service route.

Table 11. Destination Service Route Settings

Field	Description
Destination	Enter the **Destination** IP address.
Source Interface	Select the **Source Interface** that will be used for packets returning from the destination.
Source Address	Select the **Source Address** that will be used for packets returning from the destination. You do not need to enter the subnet for the destination address.

Defining a DNS Server Profile

▶ *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.

Table 12 describes the DNS server profile settings.

Table 12. DNS Server Profile Settings

Field	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	Click the check box 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	Click the check box 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.

Defining Content-ID Settings

▶ *Device > Setup > Content-ID*

Use the **Content-ID** tab to define settings for URL filtering, data protection, and container pages.

Table 13. Content-ID Settings

Function	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 information on URL filtering, see “URL Filtering Profiles”.
URL Continue Timeout	Specify the interval in minutes following a user's “continue” action before the user must press continue again for URLs in the same category (range is 1-86400, default is 15).

Table 13. Content-ID Settings (Continued)

Function	Description
URL Admin Override Timeout	Specify the interval in minutes after the user enters the admin override password before the user must re-enter the admin override password for URLs in the same category (range is 1-86400, default is 900).
URL Admin Lockout Timeout	Specify the period of time in minutes that a user is locked out from attempting to use the URL Admin Override password following three unsuccessful attempts (range is 1-86400, default is 1800).
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 server(s) on your network. You can enter up to 20 entries. The firewall connects to the public PAN-DB cloud, by default. The private PAN-DB solution is for enterprises that disallow the firewall(s) from directly accessing the PAN-DB servers in the public cloud. The firewalls access the servers included in this PAN-DB server(s) 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, click **Add** and specify the settings that apply when a URL filtering profile blocks a page and the **Override** action is specified (for details, see “URL Filtering Profiles”): • **Location**—Select the virtual system from the drop-down list (multi-vsys firewalls only). • **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 “Managing SSL/TLS Service Profiles”. • **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**, enter the IP address for redirection. Click ☒ to delete an entry.
Content-ID Settings	
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. The range is 1-50, default is 5.
Allow Forwarding of Decrypted Content	Select the check box to allows the firewall to forward decrypted content to an outside service. When selected, this allows the firewall to forward decrypted content when port mirroring or sending WildFire files for analysis. For device with multiple virtual system capability, this option is enabled for each virtual system. To enable this setting for each virtual system, go to the **Device > Virtual Systems** tab.

Table 13. Content-ID Settings (Continued)

Function	Description
X-Forwarded-For Headers	
Use X-Forwarded-For Header in User-ID	Select this check box to specify that the User-ID service 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 the IP addresses of users. The User-ID service 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 an invalid IP address, the User-ID service uses that IP address as a username for group mapping references in policies. If the header has multiple IP addresses, the User-ID service uses the first entry from the left. URL logs display the matched usernames in the Source User field. If the User-ID service 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.
Strip-X-Forwarded-For Header	Select this check box 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. **Note:** *Selecting this check box doesn't disable the use of XFF headers for user attribution in policies (see "Use X-Forwarded-For Header in User-ID"); the firewall zeroes out the XFF value only after using it for user attribution.*
Content-ID Features	
Manage Data Protection	Add additional protection for access to logs that may contain sensitive information, such as credit card numbers or social security numbers. Click **Manage Data Protection** and configure the following: • To set a new password if one has not already been set, click **Set Password**. Enter and confirm the password. • To change the password, click **Change Password**. Enter the old password, and enter and confirm the new password. • To delete the password and the data that has been protected, click **Delete Password**.
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 list. If a virtual system does not have an explicit container page defined, the default content types are used. Click **Add** and enter or select a 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.

Configuring WildFire Settings

▶ *Device > Setup > WildFire*

Use the **WildFire** tab to configure WildFire settings on the firewall. 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, you need to select the "Allow Forwarding of Decrypted Content" check box in **Device > Setup > Content-ID > URL Filtering** Settings box.*

Table 14. WildFire Settings on the Firewall

Field	Description
General Settings	
WildFire Public Cloud	Enter **wildfire.paloaltonetworks.com** to use the WildFire cloud hosted in the United States to analyze files. To use the WildFire cloud hosted in Japan, enter wildfire.paloaltonetworks.jp. You may want to use the Japan server if you do not want benign files forwarded to the U.S. cloud servers. If a file sent to the Japan cloud is determined to be malicious, the Japan cloud system forwards it to the U.S. servers where the file is reanalyzed and a signature is generated. If you are in the Japan region, you might also experience faster response times for sample submissions and report generation.
WildFire Private Cloud	Specify the IP address or FQDN of the WildFire appliance to be used to analyze files.
Maximum File Size (MB)	Specify the maximum file size that will be forwarded to the WildFire server. Available ranges are: • flash (Adobe Flash)—1-10MB, default 5MB • apk (Android Application)—1-50MB, default 10MB • pdf—(Portable Document Format) 100KB-1000KB, default 200KB • jar (Packaged Java class file)—1-10MB, default 1MB • pe (Portable Executable)—1-10MB, default 2MB • ms-office (Microsoft Office)—200KB-10000KB, default 500KB **Note:** *The values listed above may differ based on the version of PAN-OS and/or the content release version that is installed. To view the valid ranges, click in the Size Limit field and a pop-up will appear showing the available range and default value.*
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. **Note:** *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.*

Table 14. WildFire Settings on the Firewall (Continued)

Field	Description
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. **Note:** *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.*
Session Information Settings	
Settings	Specify the information to be forwarded to the WildFire server. By default, all are selected: • **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.

Defining Session Settings

▶ *Device > Setup > Session*

Use the **Session** tab 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”
- “Decryption Settings: Certificate Revocation Checking”
- “Decryption Settings: Forward Proxy Server Certificate Settings”
- “VPN Session Settings”

Session Settings

Table 15. Session Settings

Field	Description
Rematch Sessions	Click **Edit** and select **Rematch Sessions** to cause the firewall to apply newly configured security policies to sessions that are already in progress. This capability is enabled by default. If this setting is disabled, any policy change applies only to sessions initiated after the policy change was committed. For example, if a Telnet session started while an associated policy was configured that allowed Telnet, and you subsequently committed a policy change to deny Telnet, the firewall applies the revised policy to the current session and blocks it.
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 10-65535 packets, default 100).
ICMPv6 Error Packet Rate	Enter the average number of ICMPv6 error packets per second allowed globally through the firewall (range is 10-65535 packets/second, default is 100 packets/second). 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, click **Edit** and select the **IPv6 Firewalling** check box. All IPv6-based configurations are ignored if IPv6 is not enabled. Even if IPv6 is enabled for an interface, the **IPv6 Firewalling** setting must also be enabled for IPv6 to function.
Enable Jumbo Frame Global MTU	Select to enable jumbo frame support on Ethernet interfaces. Jumbo frames have a maximum transmission unit (MTU) of 9192 bytes and are available on certain platforms. • If you do not check **Enable Jumbo Frame**, the **Global MTU** defaults to 1500 bytes; the range is 576 to 1500 bytes. • If you check **Enable Jumbo Frame**, the **Global MTU** defaults to 9192 bytes; the range is 9192 to 9216 bytes. If you enable jumbo frames and you have interfaces where the MTU is not specifically configured, those interfaces will automatically inherit the jumbo frame size. Therefore, before you enable jumbo frames, if you have any interface that you do not want to have jumbo frames, you must set the MTU for that interface to 1500 bytes or another value. To configure the MTU for the interface (**Network > Interfaces > Ethernet**), see “Layer 3 Interface Settings”.
NAT64 IPv6 Minimum Network MTU	Enter the global MTU for IPv6 translated traffic. The default of 1280 bytes is based on the standard minimum MTU for IPv6 traffic.

Table 15. Session Settings (Continued)

Field	Description
NAT Oversubscription Rate	Select the DIPP NAT oversubscription rate, which is the number of times that the same translated IP address and port pair can be used concurrently. Reducing the oversubscription rate will decrease the number of source device translations, but will provide higher NAT rule capacities. • **Platform Default**—Explicit configuration of the oversubscription rate is turned off; the default oversubscription rate for the platform applies. See platform default rates at https://www.paloaltonetworks.com/products/product-selection.html. • **1x**—1 time. This means no oversubscription; each translated IP address and port pair can be used only once at a time. • **2x**—2 times • **4x**—4 times • **8x**—8 times
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 between 1-65535 messages per second.
Accelerated Aging	Enables accelerated aging-out of idle sessions. Select the check box 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 of one-half the time. To calculate the session's accelerated aging, 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 3600 seconds would time out 10 times faster (in 1/10 of the time), which is 360 seconds.

Session Timeouts

A session timeout defines 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.

On the firewall, you can define a number of timeouts for TCP, UDP, and ICMP 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 or UDP session timeouts.

Use the options in this section to configure global session timeout settings—specifically for TCP, UDP and ICMP, and for all other types of sessions.

The defaults are optimal 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.

Table 16. Session Timeouts

Field	Description
Default	Maximum length of time that a non-TCP/UDP or non-ICMP session can be open without a response. Default is 30 seconds; range is 1-1599999 seconds
Discard Timeouts	PAN-OS applies the discard timeout when denying a session based on security policies configured on the firewall.
– Discard Default	Applies only to non-TCP/UDP traffic. Default is 60 seconds; range is 1-1599999 seconds
– Discard TCP	Applies to TCP traffic. Default is 90 seconds; range is 1-1599999 seconds
– Discard UDP	Applies to UDP traffic. Default is 60 seconds; range is 1-1599999 seconds
ICMP	Maximum length of time that an ICMP session can be open without an ICMP response. Default is 6 seconds; range is 1-1599999 seconds
Scan	Maximum length of time that any session remains open after it is considered inactive. PAN-OS regards an application as inactive when it exceeds the trickling threshold defined for the application. Default is 10 seconds; range is 5-30 seconds
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). Default is 3600 seconds; range is 1-1599999 seconds
TCP handshake	Maximum length of time between receiving the SYN-ACK and the subsequent ACK to fully establish the session. Default is 10 seconds; range is 1-60 seconds
TCP init	Maximum length of time between receiving the SYN and SYN-ACK before starting the TCP handshake timer. Default: 5 seconds; range is 1-60 seconds
TCP Half Closed	Maximum length of time between receiving the first FIN and receiving the second FIN or a RST. Default: 120 seconds; range is 1-604800 seconds
TCP Time Wait	Maximum length of time after receiving the second FIN or a RST. Default: 15 seconds; range is 1-600 seconds
Unverified RST	Maximum length of time 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). Default: 30 seconds; range is 1-600 seconds
UDP	Maximum length of time that a UDP session remains open without a UDP response. Default is 30 seconds; range is 1-1599999 seconds

Table 16. Session Timeouts (Continued)

Field	Description
Captive Portal	The authentication session timeout in seconds for the Captive Portal web form (default is 30, range is 1-1,599,999). To access the requested content, the user must enter the authentication credentials in this form and be successfully authenticated. To define other Captive Portal timeouts, such as the idle timer and the expiration time before the user must be re-authenticated, use the **Device > User Identification > Captive Portal Settings** tab. See "Captive Portal Settings Tab".

Decryption Settings: Certificate Revocation Checking

In the **Session** tab, Decryption Settings section, select **Certificate Revocation Checking** to set the parameters described in the following table.

Table 17. Session Features: Certificate Revocation Checking

Field	Description
Enable: CRL	Select this check box 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 "Decryption Policies".
Receive Timeout: CRL	If you enabled the CRL method for verifying certificate revocation status, specify the interval in seconds (1-60, default 5) after which the firewall stops waiting for a response from the CRL service.
Enable: OCSP	Select the check box 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 (1-60, default 5) after which the firewall stops waiting for a response from the OCSP responder.
Block Session With Unknown Certificate Status	Select the check box 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 the check box to block SSL/TLS sessions after the firewall registers a CRL or OCSP request timeout. Otherwise, the firewall proceeds with the session.

Table 17. Session Features: Certificate Revocation Checking (Continued)

Field	Description
Certificate Status Timeout	Specify the interval in seconds (1-60, default 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 the **Session** tab, Decryption Settings section, select **Forward Proxy Server Certificate Settings** to configure the **Key Size** and hashing algorithm of the certificates that the firewall presents to clients when establishing sessions for SSL/TLS Forward Proxy decryption. The following table describes the parameters.

Table 18. Session Features: Forward Proxy Server Certificate Settings

Field	Description
Defined by destination host	Select this option if you want PAN-OS to generate certificates based on the key that the destination server uses: • If the destination server uses an RSA 1024-bit key, PAN-OS generates a certificate with that key size and an SHA-1 hashing algorithm. • If the destination server uses a key size larger than 1024 bits (for example, 2048 bits or 4096 bits), PAN-OS generates a certificate that uses a 2048-bit key and SHA-256 algorithm. This is the default setting.
1024-bit RSA	Select this option if you want PAN-OS to generate certificates that use an RSA 1024-bit key and SHA-1 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 2048 bits. In the future, depending on its security settings, when presented with such keys the browser might warn the user or block the SSL/TLS session entirely.
2048-bit RSA	Select this option if you want PAN-OS to generate certificates that use an RSA 2048-bit key and SHA-256 hashing algorithm regardless of the key size that the destination server uses. Public CAs and popular browsers support 2048-bit keys, which provide better security than the 1024-bit keys.

VPN Session Settings

In the **Session** tab, in the VPN Session Settings section, configure global settings related to the firewall establishing a VPN session. The following table describes the settings.

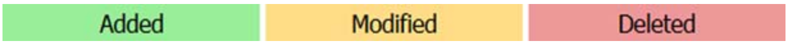
Table 19 VPN Session Settings

Field	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: 0-65535. Default: 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: 1-65535. Default: 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: 1-4000. Default: 500.

Comparing Configuration Files

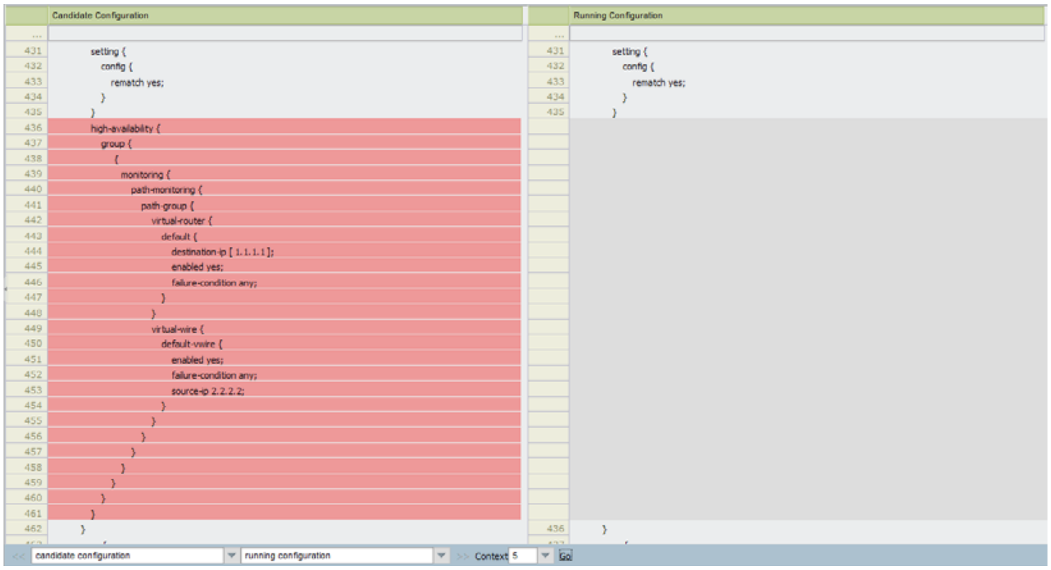
▶*Device > Config Audit*

You can view and compare configuration files by using the **Config Audit** page. From the drop-down lists, select the configurations to compare. Select the number of lines that you want to include for context, and click **Go**. 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):



The page also includes << and >> buttons adjacent to the drop-down lists, which are enabled when comparing two consecutive configuration versions. Click << to change the configurations being compared to the previous set of stored configurations, and click to >> to change the configurations being compared to the next set of stored configurations.

Figure 1. Configuration Comparison



Candidate Configuration

```
        setting {
          config {
            rematch yes;
          }
        }
        high-availability {
          group {
            {
              monitoring {
                path-monitoring {
                  path-group {
                    virtual-router {
                      default {
                        destination-ip [ 1.1.1.1 ];
                        enabled yes;
                        failure-condition any;
                      }
                    }
                    virtual-wire {
                      default-vwire {
                        enabled yes;
                        failure-condition any;
                        source-ip 2.2.2.2;
                      }
                    }
                  }
                }
              }
            }
          }
        }
      }
```

Running Configuration

```
        setting {
          config {
            rematch yes;
          }
        }
      }
```

candidate configuration running configuration Context 5

Panorama automatically saves all of the configuration files that are committed on each managed firewall, whether the changes are made through the Panorama interface or locally on the firewall.

Installing a License

▶ *Device > Licenses*

Use this page to activate licenses on all firewall platforms. 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:** To enable purchased subscriptions that require an authorization code and have been activated on the support portal, click **Retrieve license keys from license server**.

- **Activate feature using authorization code:** To enable purchased subscriptions that require an authorization code and have not been previously activated on the support portal, click **Activate feature using authorization code**. 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, follow these steps:

  a. Download the license key file from *https://support.paloaltonetworks.com*, and save it locally.

  b. Click **Manually upload license key**, click **Browse** and select the file, and 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 click **Download** to retrieve the initial seed database first and then click **Activate**.

You can also run the request url-filtering download paloaltonetworks region <region name> CLI command.

If you are unable to login to the support site listed above, go to https://www.paloaltonetworks.com/support/tabs/overview.html for support.

- **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 allow 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.

  On deactivating the license, the functionality of the firewall is disabled and it is 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 the **Export license token** link to save the token file to your local computer and then reboot the firewall. Log in to the Palo Alto Networks Support portal and access the Assets > Devices page, and click the Deactivate VM link to use this token file and complete the deactivation process.

Note: *If you are unable to access the Palo Alto Networks Support portal, go to https://www.paloaltonetworks.com/support/tabs/overview.html for additional information and support.*

  – Click **Continue** if 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.

Behavior on License Expiry

Contact the Palo Alto Networks operations team or sales for information on renewing your licenses/subscriptions.

- If the Threat Prevention subscription on the firewall expires, the following will occur:
  - A system log entry is generated; the entry states that the subscription has expired.
  - All threat prevention features will continue to function using the signatures that were installed at the time the license expired.
  - New signatures cannot be installed until a valid license is installed. Also, the ability to roll back to a previous version of the signatures is not supported if the license is expired.
  - Custom App-ID™ signatures will continue to function and can be modified.
- If the support license expires, threat prevention and threat prevention updates will continue to function normally.
- If your support entitlement expires, software updates will no be available. You will need to renew your license to continue access to software updates and to interact with the technical support group.
- If a term-based VM capacity license expires, you cannot obtain software or content updates on the firewall until you renew the license. Although you might have a valid subscription (threat prevention or WildFire, for example) and support license, you must have a valid capacity license to obtain the latest software or content updates.

Defining VM Information Sources

▶ ***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 or the Amazon Web Services, Virtual Private Cloud (AWS-VPC). There are two ways to monitor VM Information Sources:

- The firewall can monitor the VMware ESXi server, VMware vCenter server and the AWS-VPC environments 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 multiple virtual systems capable firewall, you can configure up to 10 sources.

  If your firewalls are configured in a high availability configuration:

  - in an active/passive setup, only the active firewall monitors the VM information sources.
  - in an active/active setup, only the firewall with the priority value of primary monitors the VM 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 user mapping, you can either configure the VM Information Sources on 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. Up to 100 sources are supported on the Windows User-ID agent; support for AWS is not available for the User-ID agent.

Note: *Each VM on a monitored ESXi or vCenter server must have VMware Tools installed and running. VMware Tools provide the capability to glean the IP address(es) and other values assigned to each VM.*

In order to collect the values assigned to the monitored VMs, the firewall monitors the following attributes:

Attributes Monitored on a VMware Source	Attributes Monitored on the AWS-VPC
• UUID • Name • Guest OS • VM State — the power state can be poweredOff, poweredOn, standBy, and unknown. • Annotation • 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, Host IP address.	• Architecture • Guest OS • Image ID • Instance ID • Instance State • Instance Type • Key Name • Placement—Tenancy, Group Name, Availability Zone • Private DNS Name • Public DNS Name • Subnet ID • Tag (key, value) (up to5 tags supported per instance • VPC ID

Add—To add a new source for VM Monitoring, click **Add** and then fill in the details based on the source being monitored:

- For VMware ESXi or vCenter Server see "Enabling VM Information Sources for VMware ESXi or vCenter Server".
- For AWS-VPC, see "Enabling VM Information Sources for AWS VPC".

Refresh Connected—Click to refresh the connection status; it refreshes the onscreen display. This button does not refresh the connection between the firewall and the monitored sources.

Delete—Select a configured VM Information source and click to remove the configured source.

Table 20. Enabling VM Information Sources for VMware ESXi or vCenter Server

Field	Description
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** check box 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. (default: 2 hours, range 2-10 hours) (Optional) To change the default value, select the check box to **Enable timeout when the source is disconnected** and specify the value. When the specified limit is reached or if the host is inaccessible or 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 at which the firewall retrieves information from the source. (default 5 seconds, range is 5-600 seconds)

Table 21. Enabling VM Information Sources for AWS VPC

Field	Description
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.

Table 21. Enabling VM Information Sources for AWS VPC (Continued)

Field	Description
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** check box 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
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 at which the firewall retrieves information from the source. (default 60 seconds, range is 60-1200 seconds)
Timeout	The interval in hours after which the connection to the monitored source is closed, if the host does not respond. (default 2 hours) (Optional) Select the check box to **Enable timeout when the source is disconnected**. When the specified limit is reached or if the source is inaccessible or 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. If your account is configured to use a default VPC, the default VPC ID will be listed under AWS Account Attributes.

Installing the Software

▶ *Device > Software*

Use this page to view the available software releases, download or upload a release, install a release (a support license is required), delete a software image from the device, or view release notes. Make sure to review the following recommendations before upgrading or downgrading the software version:

- Review the **Release Notes** to view a description of the changes in a release and to view the migration path to install the software.

- Save a backup your current configuration since a feature release may migrate certain configurations to accommodate new features. (Click **Device > Setup > Operations** tab and select **Export named configuration snapshot**, select **running-config.xml** and then click **OK** to save the configuration file to your computer.)
- When downgrading, it is recommended that you downgrade into a configuration that matches the software version.
- When upgrading a high availability (HA) pair to a new feature release (where the first or second digit in the PAN-OS version changes, for example from 5.0 to 6.0 or from 6.0 to 6.1), the configuration might be migrated to accommodate new features. If session synchronization is enabled, sessions will not be synchronized if one device in the cluster is running a different PAN-OS feature release.
- If you need to upgrade a firewall to a PAN-OS maintenance release for which the base release is higher than the currently installed software, you must download (without installing) the base release to the firewall before downloading and installing the maintenance release. For example, to upgrade a firewall from PAN-OS 5.0.12 to PAN-OS 6.0.3, download (without installing) PAN-OS 6.0.0 to the firewall before downloading and installing PAN-OS 6.0.3.
- The date and time settings on the firewall must be current. PAN-OS software is digitally signed and the device checks the signature before installing a new version. If the date setting on the device is not current, the device might perceive the software signature to be erroneously in the future and will display the 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.

Table 22. Software Options

Field	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.

Table 22. Software Options (Continued)

Field	Description
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 the link to initiate the download. • **Install**—The corresponding software version has been downloaded or uploaded to the firewall. Click the link to install the software. A reboot is required to complete the upgrade process. • **Reinstall**—The corresponding software version has been installed. To reinstall the same version, click the link.
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 button	Checks whether a new software update is available from Palo Alto Networks.
Upload button	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 Software Update site, download the update to that computer, and in the **Device** > **Software** page of the firewall click **Upload** to import the software image. In a high availability (HA) configuration, you can select the **Sync To Peer** check box 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** links for uploaded and downloaded software. **Release Notes** links are not available for uploaded software.

Updating Threat and Application Definitions

▶ *Device > Dynamic Updates*

▶ *Panorama > Dynamic Updates*

Palo Alto Networks regularly posts updates for application detection, threat protection, and GlobalProtect data files through dynamic updates as follows:

- **Antivirus—**Includes new and updated antivirus signatures, including signatures discovered by WildFire. You must have a Threat Prevention subscription to get these updates. New antivirus signatures are published daily.

- **Applications—**Includes new and updated application signatures. This update does not require any additional subscriptions, but it does require a valid maintenance/support contract. New application updates are published weekly.

- **Applications and Threats—**Includes new and updated application and threat signatures. This update is available if you have a Threat Prevention subscription (and in this case you will get this update instead of the Applications update). New Applications and Threats updates are published weekly. You can also choose to install only the new threat signatures in a content release version. You are prompted with this option both when installing a content release and when setting the schedule to automatically install content release versions. This option allows you to benefit from new threat signatures immediately; you can then review the policy impact for new application signatures and make any necessary policy updates before enabling them.

- **GlobalProtect Data File—**Contains the vendor-specific information for defining and evaluating host information profile (HIP) data returned by GlobalProtect agents. You must have a GlobalProtect gateway subscription in order to receive these updates. In addition, you must create a schedule for these updates before GlobalProtect will function.

- **BrightCloud URL Filtering—**Provides updates to the BrightCloud URL Filtering database only. You must have a BrightCloud subscription to get these updates. New BrightCloud URL database updates are published daily. If you have a PAN-DB license, scheduled updates are not required as devices remain in-sync with the servers automatically.

- **WildFire—**Provides near real-time malware and antivirus signatures created as a result of the analysis done by the WildFire cloud service. Without the subscription, you must wait 24 to 48 hours for the signatures to roll into the Applications and Threat update.

- **WF-Private—**Provides near real-time malware and antivirus signatures created as a result of the analysis done by a WildFire appliance (WF-500). To receive content updates from a WF-500, the firewall and appliance must both be running PAN-OS 6.1 or later and the firewall must be configured to use the WildFire appliance for file/email-link analysis.

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.

If you are managing your firewalls using Panorama and want to schedule dynamic updates for one or more firewalls, see "Scheduling Dynamic Updates".

The following table provides help for using this page.

Table 23. Dynamic Updates Options

Field	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.

Table 23. Dynamic Updates Options (Continued)

Field	Description
Schedule	Allows you to schedule the frequency for retrieving updates. You can define how often and when the dynamic content updates occur—day or date, and time—whether the updates and downloaded only or whether the updates are downloaded and installed on the firewall. When scheduling recurring downloads and installations for content updates, you can choose 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 policy updates that might be necessary for applications that are newly-identified and possibly treated differently following the update. (To later enable applications that are automatically disabled for scheduled content updates, select the **Apps, Threats** link on the Dynamic Updates page or select **Objects > Applications**). When scheduling updates, if you want to delay installing a new update until after it has been released for a certain number of hours, you can specify how long after a release to wait before performing a content update. Entering the number of hours to wait in the **Threshold (Hours)** field.
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 a link 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.

Table 23. Dynamic Updates Options (Continued)

Field	Description
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 the link to initiate the download. If the firewall does not have access to the Internet, use an Internet-connected computer to go to the Dynamic Updates site to look for and **Download** the content release version to your local computer. Then click the **Upload** button to 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. • **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; policy changes for pending applications do not take effect until the corresponding content release version is installed. • **Install**—The corresponding content release version has been downloaded to the firewall. Click the link 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 the **Apps, Threats** link 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 the link.
Documentation	Provides a link to the release notes for the corresponding version.
☒	Remove the previously downloaded content release version from the firewall.

Administrator Roles, Profiles, and Accounts

When you create an administrative account, you specify one of the following options to determine how the firewall authenticates administrative users who log in:

- **Local database—**The user login and password information is entered directly into the firewall database.
- **Client Certificate—**Existing client certificates authenticate users.

- **Authentication profile**—You select an existing external server of one of the following types to authenticate users:
  - **RADIUS** (Remote Authentication Dial-in User Service)
  - **TACACS+** (Terminal Access Controller Access-Control System Plus)
  - **LDAP** (Lightweight Directory Access Protocol)
  - **Kerberos**

Roles that you assign to administrator accounts determine the functions that the firewall allows administrators to perform after logging in. You can assign predefined roles or custom role profiles, which specify detailed privileges. For more information, see:

- "Setting Up Authentication Profiles"
- "Defining Administrator Roles"
- "Creating Administrative Accounts"
- "GlobalProtect Settings"—For information on authentication in SSL virtual private networks (VPNs)
- "Specifying Access Domains for Administrators"—For instructions on defining virtual system domains for administrators
- "Creating a Certificate Profile"—For instructions on defining certificate profiles for administrators

Defining Administrator Roles

▶ *Device > Admin Roles*

Use the **Admin Roles** page to define role profiles that determine the access and responsibilities available to administrative users. For instructions on adding administrator accounts, see "Creating Administrative Accounts".

There are also three pre-defined Admin Roles that can be used for common criteria purposes. You first use the superuser role for the initial configuration of the device and to create the administrator accounts for the Security Administrator, Audit Administrator, and Cryptographic Administrator. Once the accounts are created and the proper common criteria Admin Roles are applied, you then login using those accounts. The default superuser account in Federal Information Processing Standard (FIPS) or Common Criteria (CC) mode is **admin** and has a default password of **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 (e.g. creating the firewall's security policy) not addressed by the other two administrative roles.

To add an admin role, click **Add** and fill in the following information:

Table 24. Administrator Role Settings

Field	Description
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	Enter an optional description of the role (up to 255 characters).
Role	Select the scope of administrative responsibility: device or a virtual system (for devices enabled for multi virtual system capability).
WebUI	Click the icons for specified areas to indicate the type of access permitted for the web interface: • **Enable**—Read/write access to the selected tab. • **Read Only**—Read only access to the selected tab. • **Disable**—No access to the selected tab.
XML API	Click the icons for specified areas to indicate the type of access permitted for the XML API.
Command Line	Select the type of role for CLI access: • **None**—Access to the device CLI not permitted. • **superuser**—Full access to the current device. • **superreader**—Read-only access to the current device. • **deviceadmin**—Full access to a selected device, except for defining new accounts or virtual systems. • **devicereader**—Read-only access to a selected device.

Defining Password Profiles

▶ *Device > Password Profiles* and *Panorama > Password Profiles*

Password profiles allow you to set basic password requirements for an individual local account. If you have enabled Minimum Password Complexity (Refer to "Minimum Password Complexity"), which provides password requirements for all local accounts, this password profile will override those settings.

To create a password profile, click **Add** and enter the following information:

Table 25. Password Profile Settings

Field	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 the number of days set, ranging from 0-365 days. 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 0-30 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 0-30 days).
Post Expiration Admin Login Count	Allow the administrator to log in the 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 0-3 logins).
Post Expiration Grace Period (days)	Allow the administrator to log in the specified number of days after their account has expired (range is 0-30 days).

To apply a password profile to an account, select **Device > Administrators** (for firewalls) or **Panorama > Administrators**, select an account and then choose the profile from the **Password Profile** drop-down.

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.

Table 26. Valid Characters for Usernames and Passwords

Account Type	Restrictions
Password Character Set	There are no restrictions on any password field character sets.
Remote Admin, SSL-VPN, or Captive 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 (-) **Note:** *Login names cannot start with a hyphen (-).*

Creating Administrative Accounts

▶ *Device > Administrators*

Administrator accounts control access to devices. 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. (For details on Panorama administrators, see “Creating Panorama Administrative Accounts”.)

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 device.

- Public key authentication (SSH)—The administrator generates a public/private key pair on the machine that requires access to the device, and then uploads the public key to the device to allow secure access without requiring the administrator to enter a username and password.

To ensure that the device management interface remains secure, it is recommended that you periodically change administrative passwords using a mixture of lower-case letters, upper-case letters, and numbers. You can also enforce "Minimum Password Complexity" from ***Setup > Management****.*

To add an administrator, click **Add** and fill in the following information:

Table 27. Administrator Account Settings

Field	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, or local database authentication. For details, see "Setting Up Authentication Profiles".
Use only client certificate authentication (web)	Select the check box to use client certificate authentication for web access. If you select this check box, a username and password are not required; the certificate is sufficient to authenticate access to the device.
New Password Confirm New Password	Enter and confirm a case-sensitive password for the administrator (up to 31 characters). You can also enforce "Minimum Password" from **Setup > Management**.
Use Public Key Authentication (SSH)	Select the check box 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 (1024 bits) and RSA (768-4096 bits). **Note:** *If the public key authentication fails, a username and password prompt is presented to the administrator.*

Table 27. Administrator Account Settings (Continued)

Field	Description
Role	Assign a role to this administrator. The role determines what the administrator can view and modify. If you choose **Role Based**, select a custom role profile from the drop-down. For details, see "Defining Administrator Roles". If you select **Dynamic**, you can select one of the following pre-configured roles: • **Superuser**—Full access to the current firewall. • **Superuser (read-only)**—Read-only access to the current firewall. • **Device Admin**—Full access to a selected firewall, except for defining new accounts or virtual systems. • **Device administrator (read-only)**—Read-only access to a selected firewall. • **Vsys Admin**—Full access to a selected virtual system on a specific firewall (if multiple virtual systems are enabled). • **Vsys Admin (read-only)**—Read-only access to a selected virtual system on a specific firewall.
Virtual System (Only for a firewall virtual system administrator role)	Click **Add** to select the virtual systems that the administrator can access.
Password Profile	Select the password profile, if applicable. To create a new password profile, see "Defining Password Profiles".

Specifying Access Domains for Administrators

▶ *Device > Access Domain*

▶ *Panorama > Access Domain*

Use the **Access Domain** page to specify domains for administrator access to the firewall or Panorama. On the firewall, access domains are linked to RADIUS Vendor-Specific Attributes (VSAs) and are supported only if a RADIUS server is used for administrator authentication (see "Configuring RADIUS Server Settings"). On Panorama, you can manage access domains locally or using RADIUS VSAs (see "Specifying Panorama Access Domains for Administrators").

When an administrator attempts to log in to the firewall, the firewall queries the RADIUS server for the administrator's access domain. If there is an associated domain on the RADIUS server, it is returned and the administrator is restricted to the defined virtual systems inside the named access domain on the device. If RADIUS is not used, the access domain settings on this page are ignored.

Table 28. Access Domain Settings

Field	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 click **Add** to select them. *Access Domains are only supported on devices that support virtual systems.*

Setting Up Authentication Profiles

- ▶ *Device > Authentication Profile*
- ▶ *Panorama > Authentication Profile*

Use the **Authentication Profile** page to configure authentication settings that you can apply to administrator accounts, SSL-VPN access, and Captive Portal. Palo Alto Networks devices support local database, RADIUS, TACACS+, LDAP, and Kerberos authentication services.

Tip: After you configure an authentication profile, use the `test authentication` CLI command to determine if your firewall or Panorama management server can communicate with the back-end authentication server and if the authentication request was successful. You can perform authentication tests on the candidate configuration to determine whether the configuration is correct before you commit. For details on using the `test authentication` command, see the PAN-OS 7.0 Administrator's Guide.

Table 29. Authentication Profile Settings

Field	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. **CAUTION:** *In a firewall that is in multiple virtual systems mode (multi-vsys mode), if the **Location** of the authentication profile is a vsys, 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 vsys. While you can commit an authentication profile and sequence with the same names in these cases, reference errors might occur.*
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 (for firewalls) or as Panorama. After you save the profile, you can't change its **Location**.

Table 29. Authentication Profile Settings (Continued)

Field	Description
Authentication Tab	
Type	Select the authentication type: • **None**—Do not use any authentication on the firewall. • **Local Database**—Use the authentication database on the firewall. • **RADIUS**—Use a RADIUS server for authentication. • **TACACS+**—Use a TACACS+ server for authentication. • **LDAP**—Use LDAP for authentication. • **Kerberos**—Use Kerberos for authentication.
Server Profile	If the authentication **Type** is **RADIUS**, **TACACS+**, **LDAP**, or **Kerberos**, select the authentication server profile from the drop-down. See "Configuring RADIUS Server Settings", "Configuring TACACS+ Server Settings", "Configuring LDAP Server Settings", and "Configuring Kerberos Server Settings".
Retrieve User Group	If the authentication **Type** is **RADIUS**, select the check box to use RADIUS Vendor-Specific Attributes (VSAs) to define the group that has access to the firewall.
Login Attribute	If the authentication **Type** is **LDAP**, enter an LDAP directory attribute that uniquely identifies the user and functions as the login ID for that user.
Password Expiry Warning	If the authentication **Type** is **LDAP** and 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 1 day to 255 days). Users will not be able to access the VPN if their passwords expire. **Tip:** *As a best practice, consider configuring the agents to use pre-logon connect method. This will allow users to connect to the domain to change their passwords even after the password has expired.* **Tip:** *If users allow their passwords to expire, the administrator may assign a temporary LDAP password to enable users to log in to the VPN. In this workflow, it is a best practice to set 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).* See "GlobalProtect Settings"for more details on cookie authentication and pre-logon.
User Domain and Username Modifier	The device combines the **User Domain** and **Username Modifier** values to modify the domain/username string that a user enters during login. The device uses the modified string for authentication and uses the **User Domain** value for User-ID group mapping. Select from the following options: • To send only the unmodified user input, leave the **User Domain** blank (the default) and set the **Username Modifier** to the variable **%USERINPUT%** (the 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%**. **Note:** *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 device removes any user-entered domain string. The device 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.*

Table 29. Authentication Profile Settings (Continued)

Field	Description
Kerberos Realm	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 the **Import** link, click **Browse** to locate the keytab file, and then click **OK**. A keytab contains Kerberos account information (principal name and hashed password) for the device, which is required for SSO authentication. Each authentication profile can have one keytab. During authentication, the device 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 (username/password) authentication of the specified **Type**, which doesn't have to be Kerberos. For details on creating keytabs that are valid for Palo Alto Networks devices, see the PAN-OS 7.0 Administrator's Guide. **Note:** *If the device is in Federal Information Processing Standard (FIPS) or Common Criteria (CC) mode, the algorithm has to be aes128-cts-hmac-sha1-96 or aes256-cts-hmac-sha1-96. Otherwise, you can also use des3-cbc-sha1 or arcfour-hmac. The algorithm in the keytab has to match the algorithm in the service ticket that the Ticket Granting Service issues to clients to enable SSO. Otherwise, the SSO process will fail. Your Kerberos administrator determines which algorithms the service tickets use.*
Advanced Tab	
Allow List	Click **Add** and select **all** or select the specific users and groups that are allowed to authenticate with this profile. If you don't add entries, no users can authenticate. **Note:** *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 (see "Custom Group Subtab").* To remove users or groups, select the corresponding check boxes and click **Delete**.
Failed Attempts	Enter the number of failed login attempts (1-10) that the device allows before locking out the user account. A value of 0 (default) means there is no limit. **CAUTION:** *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	Enter the number of minutes (0-60) for which the device locks out a user account after the user reaches the number of **Failed Attempts**. A value of 0 (default) means the lockout applies until an administrator manually unlocks the user account. **CAUTION:** *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.*

Creating a Local User Database

▶ *Device > Local User Database > Users*

You can set up a local database on the firewall to store authentication information for remote access users, device administrators, and captive portal users. No external authentication server is required with this configuration, so all account management is performed on the firewall or from Panorama.

Table 30. Local User Settings

Field	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 (for 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.
Enable	Select the check box to activate the user account.

Use the **Local Users** page to add user information to the local database. When configuring Captive Portal, you first create the local account, add it to a User Group and create an Authentication Profile using the new group. You then enable Captive Portal from **Device > User Authentication > Captive Portal** and select the Authentication Profile. Once this is configured, you can then create a policy from **Policies > Captive Portal**. See "Configuring the Firewall for User Identification"for more information.

Adding Local User Groups

- ▶ *Device > Local User Database > User Groups*

Use the **User Groups** page to add user group information to the local database.

Table 31. Local User Group Settings

Field	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 (for 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.

Configuring RADIUS Server Settings

- ▶ *Device > Server Profiles > RADIUS*
- ▶ *Panorama > Server Profiles > RADIUS*

Use the **RADIUS** page to configure settings for the RADIUS servers that authentication profiles reference (see "Setting Up Authentication Profiles").

Table 32. RADIUS Server Settings

Field	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 (for firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Administrator Use Only	Select this check box to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, the check box appears only if the **Location** is **Shared**.
Timeout	Enter an interval in seconds after which an authentication request times out (range is 1-30, default is 3).
Retries	Enter the number of automatic retries following a timeout before the request fails (range is 1-5, default is 3).

Table 32. RADIUS Server Settings (Continued)

Field	Description
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 device and the RADIUS server. • **Port**—Enter the server port (default is 1812) for authentication requests.

Configuring TACACS+ Server Settings

- ▶ *Device > Server Profiles > TACACS+*
- ▶ *Panorama > Server Profiles > TACACS+*

Use the **TACACS+** page to configure settings for the Terminal Access Controller Access-Control System Plus (TACACS+) servers that authentication profiles reference (see “Setting Up Authentication Profiles”).

Table 33. TACACS+ Server Settings

Field	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 (for firewalls) or as Panorama. After you save the profile, you can’t change its **Location**.
Administrator Use Only	Select this check box to specify that only administrator accounts can use the profile for authentication. For multi-vsys firewalls, the check box 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).
Use single connection for all authentication	Select the check box 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 device and the TACACS+ server. • **Port**—Enter the server port (default is 49) for authentication requests.

Configuring LDAP Server Settings

- ▶ *Device > Server Profiles > LDAP*
- ▶ *Panorama > Server Profiles > LDAP*

Use the **LDAP** page to configure settings for the LDAP servers that authentication profiles reference (see “Setting Up Authentication Profiles”).

Table 34. LDAP Server Settings

Field	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 (for firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Administrator Use Only	Select this check box to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, the check box appears only if the **Location** is **Shared**.
Servers	For each LDAP server, click **Add** and enter the host **Name**, IP address or FQDN (**LDAP Server**), and **Port** (default is 389).
Type	Choose the server type from the drop-down list.
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.
Password/Confirm Password	Specify the bind account password. The agent saves the encrypted password in the configuration file.
Bind Timeout	Specify the time limit imposed when connecting to the directory server (1-30 seconds, default 30 seconds).
Search Timeout	Specify the time limit imposed when performing directory searches (1-30 seconds, default 30 seconds).
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 1-3600, default is 60).
Require SSL/TLS secured connection	Select this check box if you want the device to use SSL or TLS for communications with the directory server. The protocol depends on the server port: • 389 (default)—TLS (Specifically, the device uses the Start TLS operation, which upgrades the initial plaintext connection to TLS.) • 636—SSL • Any other port—The device first attempts to use TLS. If the directory server doesn't support TLS, the device falls back to SSL. This check box is selected by default.

Table 34. LDAP Server Settings (Continued)

Field	Description
Verify Server Certificate for SSL sessions	Select this check box (it is cleared by default) if you want the device to verify the certificate that the directory server presents for SSL/TLS connections. The device verifies the certificate in two respects: • The certificate is trusted and valid. For the device 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 device 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 the **Require SSL/TLS secured connection** check box.

Configuring Kerberos Server Settings

▶ *Device > Server Profiles > Kerberos*

▶ *Panorama > Server Profiles > Kerberos*

Use the **Kerberos** page 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 authentication profiles (see “Setting Up Authentication Profiles”).

! *To use Kerberos authentication, your back-end Kerberos server must be accessible over an IPv4 address. IPv6 addresses are not supported.*

Table 35. Kerberos Server Settings

Field	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 (for firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Administrator Use Only	Select this check box to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, the check box 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 (default is 88) for communication with the server.

Setting Up an Authentication Sequence

▶ *Device > Authentication Sequence*

▶ *Panorama > Authentication Sequence*

In some environments, user accounts reside in multiple directories (for example, local database, LDAP, and RADIUS). An authentication sequence is a set of authentication profiles that the Palo Alto Networks device tries to use for authenticating users when they log in. The device tries the profiles sequentially from the top of the list to the bottom—applying the authentication, Kerberos single sign-on, allows list, and account lockout values for each—until one profile successfully authenticates the user. The device only denies access if all profiles in the sequence fail to authenticate. For details on authentication profiles, see "Setting Up Authentication Profiles".

Table 36. Authentication Sequence Settings

Field	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. **CAUTION:** *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 (for firewalls) or as Panorama. After you save the sequence, you can't change its **Location**.
Use domain to determine authentication profile	Select this check box (selected by default) if you want the device 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 device 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 device does not find a match, it tries the authentication profiles in the sequence in top-to-bottom order.
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**.

Scheduling Log Exports

▶ *Device > Scheduled Log Export*

You can schedule exports of logs and save them to a File Transfer Protocol (FTP) server in CSV format or use Secure Copy (SCP) to securely transfer data between the device 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:

Table 37. Scheduled Log Export Settings

Field	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).
Enabled	Select the check box to enable the scheduling of log exports.
Log Type	Select the type of log (traffic, threat, url, data, or hipmatch). 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. You can use SCP to export logs securely, or you can use FTP, which is not a secure protocol. If you are using SCP, you need to click the Test SCP server connection button 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 the check box 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	Enter the password for access to the FTP server. A password is not required if the user is “anonymous.”

Defining Logging Destinations

▶ *Device > Log Settings*

Use this page to enable the firewall to record configuration changes, system events, HIP Match logs, correlation logs (on some platforms) and to configure and enable alarms. For each log, you can enable remote logging to Panorama, and generate SNMP traps, and select a syslog profile and email server profile for sending syslog messages and email notifications.

The following table describes the remote log destinations.

Table 38. Remote Log Destinations

Destination	Description
Panorama	All log entries can be forwarded to Panorama, the Palo Alto central management appliance. To specify the address of the Panorama server, see “Defining Management Settings”.

SNMP trap	SNMP traps can be generated by severity level for system, threat, and traffic log entries, but not for configuration log entries. To define the SNMP trap destinations, see “Configuring SNMP Trap Destinations”.
Syslog	Syslog messages can be generated by severity level for system, threat, traffic, and configuration log entries. To define the syslog destinations, see “Configuring Syslog Servers”.
Email	Email notifications can be sent by severity level for system, threat, traffic, and configuration log entries. To define the email recipients and servers, see “Configuring Email Notification Settings”.

Note: *To configure logging destinations for traffic, threat and WildFire logs, see “Log Forwarding”.*

Configuration Log Settings

The Config widget allows you to define the settings for configuration log entries.

Table 39. Configuration Log Settings

Field	Description
Panorama	Select the check box to enable sending configuration log entries to the Panorama centralized management system.
SNMP Trap	To generate SNMP traps for configuration log entries, select the SNMP trap server profile. To specify new SNMP trap destinations, see “Configuring SNMP Trap Destinations”.
Email	To generate email notifications for configuration log entries, select an email profile from the drop-down. To specify a new email profile, see “Configuring Email Notification Settings”.
Syslog	To generate syslog messages for configuration log entries, select the name of the syslog server. To specify new syslog servers, see “Configuring Syslog Servers”.

System Log Settings

The system logs show system events such as HA failures, link status changes, and administrators logging in and out of the firewall. Based on the severity of the event, you can specify whether the system log entries are logged remotely with Panorama and sent as SNMP traps, syslog messages, and/or email notifications.

Table 40. System Log Settings

Field	Description
Panorama	Select the check box for each severity level of the system log entries to be sent to the Panorama centralized management system. To specify the Panorama server address, see "Defining Management Settings". The severity levels are: • **Critical**—Hardware failures, including HA failover, and link failures. • **High**—Serious issues, including dropped connections with external devices, such as syslog and RADIUS servers. • **Medium**—Mid-level notifications, such as antivirus package upgrades. • **Low**—Minor severity notifications, such as user password changes. • **Informational**—Log in/log off, administrator name or password change, any configuration change, and all other events not covered by the other severity levels.
SNMP Trap Email Syslog	Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the system log entries are sent. To define new destinations, see: • "Configuring SNMP Trap Destinations". • "Configuring Syslog Servers". • "Configuring Email Notification Settings".

Correlation Log Settings

The firewall and Panorama log correlation events when the patterns and thresholds defined in a correlation object match the network traffic patterns captured in Application Statistics, Traffic, Threat, Data Filtering, and URL Filtering logs. A correlated event gathers evidence of suspicious or unusual behavior of users or hosts on the network. For details, see "Using the Automated Correlation Engine".

To forward Correlation logs to external services, select each event severity level (described in Table 41) and select a server profile for each desired service:

- **SNMP Trap** server profile—For details, see "Configuring SNMP Trap Destinations".
- **Email** server profile—For details, see "Configuring Email Notification Settings".
- **Syslog** server profile—For details, see "Configuring Syslog Servers".

You cannot forward Correlation logs from firewalls to Panorama. Panorama generates Correlation logs based on the firewall logs it receives.

Table 41. Correlation Log Settings

Severity Level	Description
Critical	Confirms that a host has been compromised based on correlated events that indicate an escalation pattern. For example, a critical event is logged when a host that received a file with a malicious verdict by WildFire exhibits the same command-and-control activity that was observed in the WildFire sandbox for that malicious file.
High	Indicates that a host is very likely compromised based on a correlation between multiple threat events, such as malware detected anywhere on the network that matches the command-and-control activity being generated from a particular host.
Medium	Indicates that a host is likely compromised based on the detection of one or multiple suspicious events, such as repeated visits to known malicious URLs that suggests a scripted command-and-control activity.
Low	Indicates that a host is possibly compromised based on the detection of one or multiple suspicious events, such as a visit to a malicious URL or a dynamic DNS domain.
Informational	Detects an event that may be useful in aggregate for identifying suspicious activity; each event is not necessarily significant on its own.

HIP Match Log Settings

The Host Information Profile (HIP) match log settings are used to provide information on security policies that apply to GlobalProtect clients.

Table 42. HIP Match Log Settings

Field	Description
Panorama	Select the check box to enable sending configuration log entries to the Panorama centralized management system.
SNMP Trap	To generate SNMP traps for HIP match log entries, select the name of the trap destination. To specify new SNMP trap destinations, see "Configuring SNMP Trap Destinations".
Email	To generate email notifications for configuration log entries, select the name of the email settings that specify the appropriate email addresses. To specify new email settings, see "Configuring Email Notification Settings".
Syslog	To generate syslog messages for configuration log entries, select the name of the syslog server. To specify new syslog servers, see "Configuring Syslog Servers".

Defining Alarm Settings

Alarm Settings allows you to enable alarms and alarm notifications for the CLI and the web interface. It also allows you to configure notifications for these 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.

You can view the current list of alarms at any time by clicking the **Alarms** icon Alarms in the lower right corner of the web interface when the Alarm option is configured. This opens a window that lists the unacknowledged and acknowledged alarms in the current alarms log.

To acknowledge alarms, select their check boxes and click **Acknowledge**. This action moves the alarms to the Acknowledged Alarms list. The alarms window also includes paging, column sort, and refresh controls.

To add an alarm, edit the Alarm Settings section and use the following table to define an alarm:

Table 43. Alarm Log Settings

Field	Description
Enable Alarms	Enable alarms based on the events listed on this page. The Alarms button Alarms is visible only when the **Enable Alarms** check box is selected.
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 the **Alarms** icon located on the bottom right of the web interface window. This feature is only available when in the firewall is in CCEAL4 mode.
Encryption/Decryption Failure Threshold	Specify the number of encryption/decryption failures after which an alarm is generated.
Log DB Alarm Threshold (% Full)	Generate an alarm when a log database reaches the indicated percentage of the maximum size.
Security Policy Limits	An alarm is generated if a particular IP address or port hits a deny rule the number of times specified in the **Security Violations Threshold** setting within the period (seconds) specified in the **Security Violations Time Period** setting.
Security Policy Group Limits	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.

Table 43. Alarm Log Settings (Continued)

Field	Description
Selective Audit	**Note:** *These settings appear on the **Alarms** page only in Common Criteria mode.* Specify the following settings: • **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. • **Suppress Login Failure Logging**—Stops logging of failed administrator logins to the firewall. • **TLS Session Logging**—Logs the establishment of TLS sessions. • **Suppressed Administrators**—Does not generate logs for changes that the listed administrators make to the firewall configuration.

Managing Log Settings

When configured for logging, the firewall records configuration changes, system events, security threats, traffic flows, and alarms generated by the device. Use the Manage Logs page to clear logs on the device. Click the link that corresponds to the log—traffic, threat, URL, data, configuration, system, HIP Match, Alarm—you would like to clear.

Configuring SNMP Trap Destinations

▶ ***Device > Server Profiles > SNMP Trap***

▶ ***Panorama > 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). Use the **SNMP Trap** page 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 “Enabling SNMP Monitoring”.

After creating the server profile, you must specify which log types will trigger the firewall to send SNMP traps (see “Defining Logging Destinations”). For a list of the MIBs that you must load into the SNMP manager so it can interpret traps from Palo Alto Networks devices, see Supported MIBs.

Don’t delete a server profile that any system log setting or logging profile uses.

Table 44. SNMP Trap Server Profile Settings

Field	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 (for 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.
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. As a best practice, 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	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.

Table 44. SNMP Trap Server Profile Settings (Continued)

Field	Description
User	Specify a username to identify the SNMP user account (up to 31 characters). The username you configure on the device must match the username configured on the SNMP manager.
EngineID	Specify the engine ID of the device. When an SNMP manager and the device authenticate to each other, trap messages use this value to uniquely identify the device. If you leave the field blank, the messages use the device 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 devices 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 device uses the password to authenticate to the SNMP manage4. The device 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 device uses the password and Advanced Encryption Standard (AES-128) to encrypt traps. The password must be 8-256 characters and all characters are allowed.

Configuring Syslog Servers

- *Device > Server Profiles > Syslog*
- *Panorama > Server Profiles > Syslog*

To generate syslog messages for system, configuration, traffic, threat, or HIP match logs, you must specify one or more syslog servers. After you define the syslog servers, you can use them for system and configuration log entries (see “Configuration Log Settings”).

Table 45. New Syslog Server

Field	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 (for 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 of the syslog server.
Transport	Select whether to transport the syslog messages over UDP, TCP, or SSL.
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	
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 “Configuring Email Notification Settings”.
Escaping	Specify escape sequences. Use the **Escaped characters** box to list all the characters to be escaped without spaces.

You cannot delete a server that is used in any system or configuration log settings or logging profiles.

Configuring Email Notification Settings

▶ *Device > Server Profiles > Email*

▶ *Panorama > Server Profiles > Email*

To generate email messages for logs, you must configure an email profile. After you define the email settings, you can enable email notification for system and configuration log entries (see "Configuration Log Settings"). For information on scheduling email report delivery, see "Scheduling Reports for Email Delivery".

Table 46. Email Notification Settings

Field	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	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 (for firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Servers Tab	
Server	Enter a name to identify the server (1-31 characters). This field is just a label and does not have to be the host name of an existing SMTP server.
Display Name	Enter the name shown in the From field of the email.
From	Enter the From 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.
Gateway	Enter the IP address or host name of the Simple Mail Transport Protocol (SMTP) server used to send the email.
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 the settings.
Escaping	Include escaped characters and specify the escape character or characters.

You cannot delete an email setting that is used in any system or configuration log settings or logging profiles.

Configuring Netflow Settings

▶ *Device > Server Profiles > Netflow*

All firewalls support NetFlow Version 9 except the PA-4000 Series firewall and PA-7000 Series firewalls. The firewalls support only unidirectional NetFlow, not bidirectional. You can enable NetFlow exports on all interface types except HA, log card, or decrypt mirror. The firewall supports standard and enterprise (PAN-OS specific) NetFlow templates. NetFlow collectors require templates to decipher the exported fields. The firewall selects a template based on the type of data it exports: IPv4 or IPv6 traffic, with or without NAT, and with standard or enterprise-specific fields.

To configure NetFlow data exports, define a NetFlow server profile, which specifies the NetFlow servers that will receive the data and specifies export parameters. After you assign the profile to an interface (see “Configuring a Firewall Interface”), the firewall exports NetFlow data for all traffic traversing that interface to the specified servers.

Table 47. Netflow Settings

Field	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	Specify the number of **Minutes** (1-3600, default 30) or **Packets** (1-600, default 20) after which the firewall refreshes the NetFlow template to apply any changes to its fields or a change to the template selection. The required refresh frequency 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 (1-60, default 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.
Port	Specify the port number for server access (default 2055).

Configuring a DNS Server Profile

▶ *Device > Server Profiles > DNS*

Configure a DNS server profile, which is applied to a virtual systems to simplify configuration.

Table 48 DNS Server Profile

Field	Description
Name	Specify a name for the DNS server profile.
Location	Select the virtual system to which the profile applies.
Inheritance Source	(Optional) Specify the DNS server from which the profile should inherit settings.
Check inheritance source status	(Optional) If you chose a DNS server from which to inherit settings, click this link to see the status of the inheritance source.
Primary DNS	Specify the IP address of the Primary DNS server, or leave as **inherited** if you chose an Inheritance Source.
Secondary DNS	Specify the IP address of the Secondary DNS server, or leave as **inherited** if you chose an Inheritance Source.
Service Route IPv4	Click this check box if you want to specify that packets going to the DNS server are sourced from an IPv4 address. – (Optional) Specify the **Source Interface** that packets going to the DNS server will use. – Specify the IPv4 **Source Address** from which packets going to the DNS server are sourced.
Service Route IPv6	Click this check box if you want to specify that packets going to the DNS server are sourced from an IPv6 address. – (Optional) Specify the **Source Interface** that packets going to the DNS server will use. – Specify the IPv6 **Source Address** from which packets going to the DNS server are sourced.

Using Certificates

▶ *Device > Certificate Management > Certificates*

Certificates are used to encrypt data and secure communication across a network.

- “Managing Device Certificates”: Use the **Device > Certificate Management > Certificates > Device Certificates** page to manage—generate, import, renew, delete, revoke—the device certificates used for ensuring secure communication. You can also export and import the high availability (HA) key that secures the connection between the HA peers on the network.
- “Managing the Default Trusted Certificate Authorities”: Use the **Device > Certificate Management > Certificates > Default Trusted Certificate Authorities** page to view, enable, and disable the certificate authorities (CAs) that the firewall trusts.

Managing Device Certificates

▶ *Device > Certificate Management > Certificates > Device Certificates*

▶ *Panorama > Certificate Management > Certificates*

Lists the certificates that the firewall or Panorama use for tasks such as securing access to the web interface, SSL decryption, or LSVPN.

The following are some uses for certificates:

- **Forward Trust**—This certificate is presented to clients during decryption when the server to which they are connecting is signed by a CA in the firewall's trusted CA list. If a self-signed certificate is used for forward proxy decryption, you must click the certificate name in the **Certificates** page and select the **Forward Trust Certificate** check box.
- **Forward Untrust—**This certificate is presented to clients during decryption when the server to which they are connecting is signed by a CA that is not in the firewall's trusted CA list.
- **Trusted Root CA—**The certificate is marked as a trusted CA for forward decryption purposes.

  When the firewall decrypts traffic, it checks the upstream certificate to see if it is issued by a trusted CA. If not, it uses a special untrusted CA certificate to sign the decryption certificate. In this case, the user sees the usual certificate error page when accessing the firewall and must dismiss the login warning.

  The firewall has a large list of existing trusted CAs. The trusted root CA certificate is for additional CAs that are trusted for your enterprise but are not part of the pre-installed trusted list.
- **SSL Exclude—**This certificate excludes connections if they are encountered during SSL forward proxy decryption.
- **Certificate for Secure Syslog—**This certificate enables secure forwarding of syslogs to an external syslog server.

To generate a certificate, click **Generate** and fill in the following fields:

Table 49. Settings to Generate a Certificate

Field	Description
Certificate Name	Enter a name (up to 31 characters) to identify the certificate. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. Only the name is required.
Common Name	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 this check box if you want the certificate to be available to every vsys.
Signed By	A certificate can be signed by a certificate authority (CA) certificate that has been imported in to the firewall or it can be self-signed where 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 have imported CA certificates or have issued them on the device (self-signed), the drop-down includes the CAs available to sign the certificate that is being created. To generate a certificate signing request (CSR), select **External Authority (CSR)**. The device generates the certificate and the key pair and you can then export the CSR.
Certificate Authority	Select this check box 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.

Table 49. Settings to Generate a Certificate (Continued)

Field	Description
OCSP Responder	Select an OSCP responder profile from the drop-down (see “Adding an OCSP Responder”). The corresponding host name appears in the certificate.
Algorithm	Select a key generation algorithm for the certificate: **RSA** or **Elliptic Curve DSA** (ECDSA). **Note:** *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. Otherwise, select RSA for compatibility with legacy browsers and operating systems.* **WARNING:** *Firewalls that run releases before PAN-OS 7.0 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.*
Number of Bits	Select the key length for the certificate. If the firewall is in FIPS or CC mode and the key generation **Algorithm** is **RSA**, the RSA keys generated must be **2048** bits or larger. 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 or 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.
Expiration (days)	Specify the number of days that the certificate will be valid. The default is 365 days. **CAUTION:** *If you specify a **Validity Period** in a GlobalProtect satellite configuration, that value will override the value entered in this field.*
Certificate Attributes	Optionally click **Add** to specify additional **Certificate Attributes** to use to identify the entity to which you are issuing the certificate. You can add any of the following attributes: **Country**, **State**, **Locality**, **Organization**, **Department**, **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). **Note:** *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.

After you generate the certificate, the details display on the page.

Table 50. Other Supported Actions

Actions	Description
Delete	Select the certificate to delete and click **Delete.**
Revoke	Select the certificate that you want to revoke, and click **Revoke**. The certificate will be instantly set to the **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 Open Certificate Status Protocol (OCSP) to verify certificate revocation status, the firewall uses the OCSP responder information to update the certificate status
Import	To import a certificate, click **Import** and configure the fields 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. • Select the **File Format** for the certificate. • Select the **Private key resides on Hardware Security Module** check box if an HSM stores the key for this certificate. For HSM details, see "Defining Hardware Security Modules". • Select the **Import private key** check box if you want to import the private key also. 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**.
Generate	See generate.
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 the **Export Private Key** check box and enter a **Passphrase** and **Confirm Passphrase**. • **Binary Encoded Certificate (DER)**—You can export only the certificate, not the key: ignore the **Export Private Key** check box and passphrase fields.

Table 50. Other Supported Actions

Actions	Description
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 link for the certificate and select the check boxes to indicate how you plan to use the certificate. For a description of each, see uses.

Managing the 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. For each CA, the name, subject, issuer, expiration date and validity status is displayed.

This list does not include the CA certificates generated on the firewall.

Table 51 Trusted Certificate Authorities Settings

Field	Description
Enable	If you have disabled a CA and want to enable it, click the check box next to the CA and then click **Enable**.
Disable	Click the check box next to the CA that you want to disable, then click **Disable**. This may be desired if you only want to trust certain CAs, or remove all of them to only trust your local CA.
Export	Click the check box next to the CA, then click **Export** to export the CA certificate. You can do this to import into another system, or if you want to view the certificate offline.

Creating a Certificate Profile

▶ *Device > Certificate Management > Certificate Profile*

▶ *Panorama > Certificate Management > Certificate Profiles*

Certificate profiles define user and device authentication for Captive Portal, GlobalProtect, site-to-site IPSec VPN, Mobile Security Manager, and firewall/Panorama web interface access. The profiles specify which certificates to use, how to verify certificate revocation status, and how that status constrains access. Configure a certificate profile for each application.

Table 52. Certificate Profile Settings

Page Type	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.
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 (for firewalls) or as Panorama. After you save the profile, you can't change its **Location**.
Username Field	If GlobalProtect only uses certificates for portal/gateway authentication, PAN-OS 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**: PAN-OS uses the common name. • **Subject Alt**: Select whether PAN-OS uses the Email or Principal Name. • **None**: This is usually for GlobalProtect device or pre-login authentication.
Domain	Enter the NetBIOS domain so PAN-OS can map users through User-ID.
CA Certificates	Click **Add** and select a **CA Certificate** to assign to the profile. Optionally, if the firewall uses Open 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 OCSP responder URL that you set in the procedure "Adding an OCSP Responder". To override that setting, 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 for validation, select it in the **OCSP Verify CA Certificate** field.
Use CRL	Select the check box to use a certificate revocation list (CRL) to verify the revocation status of certificates.
Use OCSP	Select the check box to use OCSP to verify the revocation status of certificates. **Note:** *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 (1-60 seconds) after which the firewall stops waiting for a response from the CRL service.
OCSP Receive Timeout	Specify the interval (1-60 seconds) after which the firewall stops waiting for a response from the OCSP responder.
Certificate Status Timeout	Specify the interval (1-60 seconds) after which the firewall stops waiting for a response from any certificate status service and applies any session blocking logic you define.

Table 52. Certificate Profile Settings (Continued)

Page Type	Description
Block session if certificate status is unknown	Select the check box 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 session.
Block sessions if certificate status cannot be retrieved within timeout	Select the check box if you want the firewall to block sessions after it registers an OCSP or CRL request timeout. Otherwise, the firewall proceeds with the session.

Adding an OCSP Responder

▶ *Device > Certificate Management > OCSP Responder*

Use the **OCSP Responder** page 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**, edit the Management Interface Settings section, select **HTTP OCSP**, 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 section, enter the **Receive Timeout** (the interval after which the firewall stops waiting for an OCSP response), 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**.

Table 53 OCSP Responder Settings

Field	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.

Managing SSL/TLS Service Profiles

▶ *Device > Certificate Management > SSL/TLS Service Profile*

▶ *Panorama > Certificate Management > SSL/TLS Service Profile*

SSL/TLS service profiles specify a certificate and a protocol version or range of versions for device services that use SSL/TLS. By defining the protocol versions, the profiles enable you to restrict the cipher suites that are available for securing communication with the clients requesting the services.

To add a profile, click **Add**, complete the fields in the following table, and then click **OK**.

To clone a profile, select it, click **Clone**, and then click **OK**.

To delete a profile, select it and click **Delete**.

Table 54 SSL/TLS Service Profile Settings

Field	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), you can select this check box to make the profile available on all virtual systems. By default, the check box is cleared and the profile is available only in the vsys selected in the **Device** tab, **Location** drop-down.
Certificate	Select, import, or generate a certificate to associate with the profile. See "Managing Device Certificates". **CAUTION:** *Do not use certificate authority (CA) certificates for SSL/TLS services; use only signed certificates.*

Table 54 SSL/TLS Service Profile Settings

Field	Description
Min Version	Select the earliest TLS version that services to which this profile is assigned can use: **TLSv1.0**, **TLSv1.1**, or **TLSv1.2**.
Max Version	Select the latest TLS version that services to which this profile is assigned can use: **TLSv1.0**, **TLSv1.1**, **TLSv1.2**, or **Max** (the latest available version).

Encrypting Private Keys and Passwords on the Firewall

▶ *Device > Master Key and Diagnostics*

▶ *Panorama > Master Key and Diagnostics*

Use the **Master Key and Diagnostics** page to specify a master key to encrypt the private keys on the device (firewall or Panorama appliance). The master key is used to encrypt private keys such as the RSA key that is used to authenticate access to the CLI, the private key used to authenticate access to the web interface of the device, as well as any other keys loaded on to the device. Because the master key is used to encrypt all other keys, make sure to store the master key in a safe location.

Even if a new master key is not specified, private keys are always stored in an encrypted form on the device, by default. This master key option offers an added layer of security.

If the devices are in a high availability (HA) configuration, make sure that the same master key is used on both devices to ensure that private keys and certificates are encrypted with the same key. If the master keys are different, HA configuration synchronization will not work properly.

To add a master key, click the edit button in the Master Key section and use the following table to enter the values:

Table 55. Master Key and Diagnostics Settings

Field	Description
Current Master Key	Specify the key that is currently used to encrypt all of the private keys and passwords on the device.
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 1-730 days). You will need to update the master key before it expires. For information on updating master keys, see “Enabling HA on the Firewall”.
Time for Reminder	Specify the number of days and hours before expiration when the user is notified of the impending expiration (range 1-365 days).

Table 55. Master Key and Diagnostics Settings (Continued)

Field	Description
Stored on HSM	Check this box 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 devices in high availability mode. Therefore, each peer in an HA pair can connect to a different HSM source. If you are using Panorama and would like to keep the configuration on both peers in sync, use Panorama templates to configure the HSM source on the managed firewalls. HSM is not supported the PA-200, PA-500 and PA-2000 Series firewalls.
Common Criteria	In Common Criteria mode, additional buttons 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.

Enabling HA on the Firewall

▶ *Device > High Availability*

For redundancy, deploy your Palo Alto Networks next-generation firewalls in a high availability configuration. 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 version 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.

HA Lite

The PA-200 firewall supports HA lite, a version of active/passive HA that does not include any session synchronization. HA lite does provide configuration synchronization and synchronization of some runtime items. It also supports failover of IPSec tunnels (sessions must be re-established), DHCP server lease information, DHCP client lease information, PPPoE lease information, and the firewall's forwarding table when configured in Layer 3 mode.

For each section on the **High Availability** page, click **Edit** in the header, and specify the corresponding information described in the following table.

Table 56. HA Settings

Field	Description
General Tab	
Setup	Specify the following settings: • **Enable HA**—Activate HA functionality. • **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**—Enter a description of the HA pair (optional). • **Mode**—Set the type of HA deployment: **Active Passive** or **Active Active**. • **Device ID**—In active/active configuration, set the Device ID to determine with peer will be the active-primary (set **Device ID** to **0**) or active-secondary (set the **Device ID** to **1**). • **Enable Config Sync**—Select this check box to enable synchronization of configuration settings between the peers. As a best practice, config sync should always be enabled. • **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.
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. – **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. – **shutdown**—Forces the interface link to the down state. This is the default option, which ensures that loops are not created in the network. • **Monitor Fail Hold Down Time (min)** —This value between 1-60 minutes determines the interval in which a firewall will be in a non-functional state after a link or path monitoring failure.

Table 56. HA Settings (Continued)

Field	Description
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 0-255) when the preemptive capability is enabled on both firewalls in the pair. • **Heartbeat Backup**—Uses the management ports on the HA devices 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. • **Preemptive**—Enables the higher priority firewall to resume active (active/passive) or active-primary (active/active> operation after recovering from a failure. The Preemption option must be enabled on both devices for the higher priority firewall to resume active or active-primary operation upon recovery following a failure. If this setting is off, then the lower priority firewall remains active or active-primary even after the higher priority firewall recovers from a failure. • **HA Timer Settings**— Select one of the preset profiles: – **Recommended**: Use for typical failover timer settings – **Aggressive**: Use for faster failover timer settings. *To view the preset value for an individual timer included in a profile, select **Advanced** and click **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**—Enter the time that the passive device (in active/passive mode) or the active-secondary device (in active/active mode) will wait before taking over as the active or active-primary device after communications with the HA peer have been lost. This hold time will begin only after the peer failure declaration has been made. – **Hello Interval**—Enter the number of milliseconds between the hello packets sent to verify that the HA program on the other firewall is operational. The range is 8000-60000 ms with a default of 8000 ms for all platforms. – **Heartbeat Interval**—Specify how frequently the HA peers exchange heartbeat messages in the form of an ICMP ping (range 1000-60000 ms; no default value exists). The recommended value, for example, on the PA-2000 and below models is 2000ms. – **Maximum No. of Flaps**—A flap is counted when the firewall leaves the active state within 15 minutes after it last left the active state. You can specify the maximum number of flaps that are permitted before the firewall is determined to be suspended and the passive firewall takes over (range 0-16, default 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**—Enter the time a passive or active-secondary device will wait before taking over as the active or active-primary device (range 1-60 min, default 1 min).

Table 56. HA Settings (Continued)

Field	Description
	– **Monitor Fail Hold Up Time (ms)**—Specify the interval 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 0-60000 ms, default 0 ms). – **Additional Master Hold Up Time (min)**—This time interval is applied to the same event as Monitor Fail Hold Up Time (range 0-60000 ms, default 500 ms). 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 devices experience the same link/path monitor failure simultaneously.

Table 56. HA Settings (Continued)

Field	Description
Control Link (HA1)/ Control Link (HA1 Backup)	The recommended configuration for the HA control link connection is to use the dedicated HA1 link between the two devices and use the management port as the Control Link (HA Backup) interface. In this case, you do not need to enable the Heartbeat Backup option in the Elections Settings page. If you are using a physical HA1 port for the Control Link HA link and a data port for Control Link (HA Backup), it is recommended that enable the Heartbeat Backup option. For devices that do not have a dedicated HA port, such as the PA-200 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. Since the management port is being used in this case, there is no need to enable the Heartbeat Backup option in the Elections Settings page 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, you should be aware 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 devices that do not have a dedicated HA port, use the management port.* 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. • **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 device. The HA key on this device must also be exported from this device and imported on the HA peer. Configure this setting for the primary HA1 interface. Import/export keys on the Certificates page (refer to Creating a Certificate Profile). • **Monitor Hold Time (ms)**—Enter the length of time (milliseconds) that the firewall will wait before declaring a peer failure due to a control link failure (1000-60000 ms, default 3000 ms). This option monitors the physical link status of the HA1 port(s).

Table 56. HA Settings (Continued)

Field	Description
Data Link (HA2)	Specify the following settings for the primary and backup data link: • **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 in the HA pair 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. • **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 advantage of using a UDP mode is the presence of UDP checksum to verify the integrity of a session sync message. • **Link Speed (Models with dedicated HA ports only)**—Select the speed for the control link between peers for the dedicated HA2 port. • **Link Duplex (Models with dedicated HA ports only)**—Select a duplex option for the control link between peers for the dedicated HA2 port. • **HA2 keep-alive**—Select this check box 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 10000 ms). If you enable HA2 keep-alive, the HA2 Keep-alive recovery Action will be taken. Select one of the following **Action** settings: – **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 are, 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.

Table 56. HA Settings (Continued)

Field	Description
	– **Threshold (ms)**—The duration in which keep-alive messages have failed before the selected **Action** occurs (range 5000-60000ms, default 10000ms). **Note:** *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.*
Link and Path Monitoring Tab (Not available for the VM-Series firewall in AWS)	
Path Monitoring	Specify the following: • **Enabled**—Enable 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**—Select whether a failover occurs when any or all of the monitored path groups fail to respond.
Path Group	Define one or more path groups to monitor specific destination addresses. To add a path group, click **Add** for the interface type (virtual wire, VLAN, or virtual router) and specify the following: • **Name**—Select a virtual wire, VLAN, or virtual router from the drop-down (the drop-down is populated depending on if you are adding a virtual wire, VLAN, or virtual router path). • **Enabled**—Enable the path group. • **Failure Condition—**Select whether a failure occurs when any or all of the specified destination addresses fails to respond. • **Source IP**—For virtual wire and VLAN interfaces, enter the source IP address used in the probe packets 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. • **Destination IPs**—Enter one or more (comma-separated) destination IP addresses to monitor. • **Ping Interval**—Specify the interval between pings to the destination address (range 200-60,000 milliseconds, default 200 milliseconds). • **Ping Count**—Specify the number of failed pings before declaring a failure (range 3-10 pings, default 10 pings).

Table 56. HA Settings (Continued)

Field	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.
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 monitor.
Active/Active Config Tab	
Packet Forwarding	Select the **Enable** check box to 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. forward packets between the HA peer that performs session setup and the HA peer that owns the session in an active/active configuration as well as for forwarding packets with asymmetric routing.
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. Active/active deployments do 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. This timer defines how long it will stay in this state. During the tentative period the firewall will attempt 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 blackhole packets because it would not have the necessary routes (default 60 seconds).

Table 56. HA Settings (Continued)

Field	Description
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 recommended 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 device receives the first packet, it will forward all packets requiring Layer 7 inspection to the active-primary firewall over the HA3 link.
Session Setup	The firewall responsible for session setup performs Layer 2 through Layer 4 processing (including address translation) and creates the session table entry. Because session setup consumes management plane resources, you can select one of the following options to help distribute the load: • **Primary Device**—The active-primary firewall sets up all sessions. • **IP Modulo**—Distributes session ownership based on the parity of the source IP address. • **IP Hash**—Distributes session ownership based on a hash of the source IP address or source and destination IP address, and hash seed value if you need more randomization. • **First Packet**—The firewall that receives the first packet performs session setup, even in cases where the peer owns the session. This option minimizes traffic over the HA3 link and ensures that the management plane-intensive work of setting up the session always happens on the firewall that receives the first packet.

Table 56. HA Settings (Continued)

Field	Description
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 device 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 to determine which device will own the floating IP address. A device with the lowest value will have the highest priority. – **Device 1 Priority**—Set the priority to determine which device will own the floating IP address. A device 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. • **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.
Operational Commands	
Suspend local device Toggles as **Make local device functional**	Places the HA peer in a suspended state, and temporarily disables HA functionality on the firewall. If you suspend the currently active firewall, the other peer will take over. To place a suspended device back into a functional state, use the following operational mode CLI command: `request high-availability state functional` To test failover, you can either uncable the active (or active-primary) device or you can click this link to suspend the active device.

Important items to consider when configuring HA

- 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 versions should be the same on each device. A mismatch can prevent the devices in the pair from being synchronized.
- 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 pressing the **Push Configuration** button located in the HA widget on the **Dashboard** tab. Note that the configuration on the device from which you push the configuration overwrites the configuration on the peer device. To synchronize the firewalls from the CLI on the active device, use the command `request high-availability sync-to-remote running-config`.

In a High Availability (HA) active/passive configuration with devices that use 10 gigabit SFP+ ports, when a failover occurs and the active device 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 device 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.

Defining Virtual Systems

▶ ***Device > Virtual Systems***

Virtual systems (vsys) are independent (virtual) firewall instances 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 device and network functions while creating vsys administrator accounts that allow access to individual vsys. This allows the vsys administrator in the Finance department to manage the security policies only for that department.

Networking functions, including static and dynamic routing, pertain to an entire firewall and all its vsys; vsys do not control device- and network-level functions. 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/assign additional virtual routers and assign interfaces, VLANs, and virtual wires as needed.

If you use a Panorama template to define vsys, you can set one vsys as the default. The default vsys and Multiple Virtual Systems mode determine whether firewalls accept vsys-specific configurations during a template commit:

- Firewalls that are in Multiple Virtual Systems mode accept vsys-specific configurations for all vsys that are defined in the template.
- Firewalls that are not in Multiple Virtual Systems mode accept vsys-specific configurations only for the default vsys. Note that if you do not set a vsys as the default, these firewalls accept no vsys-specific configurations.

The PA-4000 and PA-5000 Series firewalls and the PA-7000 Series firewalls support multiple virtual systems. The PA-2000 and PA-3000 Series firewalls can support multiple virtual systems if the appropriate license is installed. The PA-500 and PA-200 firewalls do not support multiple virtual systems.

Before enabling multiple vsys, note the following:

- A vsys administrator creates and manages all items needed for policies.

- Zones are objects within vsys. Before defining a policy or policy object, select the **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 vsys (shared) or to a single vsys.
- You can configure global (to all vsys on a firewall) or vsys-specific service routes (see "Defining Services Settings").

Before defining vsys, you must first enable the multiple vsys capability on the firewall: select **Device > Setup > Management**, edit the **General Settings**, select the **Multi Virtual System Capability** check box, and click **OK**. This adds a **Device > Virtual Systems** page. Select the page, click **Add**, and specify the following information.

Table 57. Virtual System Settings

Field	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 vsys. **Note:** *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. **Note:** *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 check box to allow the virtual system to forward decrypted content to an outside service when port mirroring or sending WildFire files for analysis. For information on Decryption Port Mirroring, see Decryption Port Mirroring.
General Tab	Select a **DNS Proxy** object if you want to apply DNS proxy rules to this vsys. See "Configuring DNS Proxy". To include objects of a particular type, select the check box for that type (interface, VLAN, virtual wire, virtual router, or visible virtual system), click **Add**, and select the object from the drop-down. You can add one or more objects of any type. To remove an object, select it and click **Delete**.

Table 57. Virtual System Settings (Continued)

Field	Description
Resource Tab	Specify the resource limits allowed for this vsys: • **Sessions Limit**—Maximum number of sessions. • **Security Rules**—Maximum number of security rules. • **NAT Rules**—Maximum number of NAT rules. • **Decryption Rules**—Maximum number decryption rules. • **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. • **Captive Portal Rules**—Maximum number of captive portal (CP) 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.

Configuring Shared Gateways

▶ *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.

Table 58. Shared Gateway Settings

Field	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 check boxes for the interfaces that the shared gateway will use.

Defining Custom Response Pages

▶ *Device > Response Pages*

Custom response pages are the web pages that are displayed 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.

Table 59. Custom Response Page Types

Page Type	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.
Captive Portal Comfort Page	Page for users to verify their user name and password for machines that are not part of the domain.
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. See “File Blocking Profiles”.
File Blocking Block Page	Access blocked because access to the file is blocked.
GlobalProtect Portal Help Page	Custom help page for GlobalProtect users (accessible from the portal).
GlobalProtect Portal Login Page	Page for users who attempt to access the GlobalProtect portal.
GlobalProtect Welcome Page	Welcome page for users who attempt to log in to the GlobalProtect portal.
SSL Certificate Errors Notify Page	Notification that an SSL certificate has been revoked.
SSL Decryption Opt-out Page	User warning page indicating that this session will be inspected.
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.

Table 59. Custom Response Page Types (Continued)

Page Type	Description
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 the **Continue** button 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 of Table 1 for instructions on setting the override password.
URL Filtering Safe Search Enforcement Block Page	Access blocked by a security policy with a URL filtering profile that has the **Safe Search Enforcement** option enabled. The user will see 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.

You can perform any of the following functions under **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 the **Export** link for the type of page. Select whether to open the file or save it to disk, and select the check box if you want to always use the same option.
- To enable or disable the **Application Block** page or **SSL Decryption Opt-out** pages, click the **Enable** link for the type of page. Select or deselect the **Enable** check box.
- 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.

Viewing Support Information

▶ *Device > Support*

▶ *Panorama > Support*

The support page allows you 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 device (firewall or Panorama appliance).

Perform any of the following functions on this page:

- **Support**—Use this section to view Palo Alto Networks Customer Support contact information, view support status for the device or activate your contract 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**—This section provides a link to the Palo Alto Networks Customer Support home page, from where you can manage your cases, and a link to register the device using your support login.

- **Tech Support File**—Use the **Generate Tech Support File** link to generate a system file that the Support group can use to help troubleshoot issues that you may be experiencing with the device. After you generate the file, click **Download Tech Support File** to retrieve it 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**—Use the **Generate Stats Dump File** link to generate a set of XML reports that summarizes network traffic over the last 7 days. After the report is generated, click the **Download Stats Dump File** link to retrieve the report. The Palo Alto Networks or Authorized Partner systems engineer uses the report to generate an Application Visibility and Risk Report (AVR Report). The AVR 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 AVR Report, please contact you Palo Alto Networks or Authorized Partner systems engineer.

Chapter 4

Network Settings

Defining Virtual Wires

▶ *Network > Virtual Wires*

Use this page to define virtual wires after you have specified two virtual wire interfaces on the firewall.

Table 60. Virtual Wire Settings

Field	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.

Table 60. Virtual Wire Settings (Continued)

Field	Description
Tags Allowed	Enter the tag number (0 to 4094) or range of tag numbers (tag1-tag2) for the traffic allowed on the virtual wire. A tag value of zero indicates untagged traffic (the default). Multiple tags or ranges must be separated by commas. Traffic that has an excluded tag value is dropped. Note that 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 this option 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 this check box if you want to bring down the other port in a virtual wire when a down link state is detected. If this check box is not selected, link status is not propagated across the virtual wire.

Configuring a Firewall Interface

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”*

What are you looking for?	See
I already understand firewall interfaces; how can I find information on configuring a specific interface type?	**Physical Interfaces (Ethernet)** ▶ *"Configure a Layer 2 Interface"* ▶ *"Configure a Layer 2 Subinterface"* ▶ *"Configure a Layer 3 Interface"* ▶ *"Configure a Layer 3 Subinterface"* ▶ *"Configure a Virtual Wire Interface"* ▶ *"Configure a Virtual Wire Subinterface"* ▶ *"Configure a Tap Interface"* ▶ *"Configure a Log Card Interface"* ▶ *"Configure a Log Card Subinterface"* ▶ *"Configure a Decrypt Mirror Interface"* ▶ *"Configure an Aggregate Interface Group"* ▶ *"Configure an Aggregate Interface"* ▶ *"Configure an HA Interface"* **Logical Interfaces** ▶ *"Configure a VLAN Interface"* ▶ *"Configure a Loopback Interface"* ▶ *"Configure a Tunnel Interface"*
Looking for more?	**See** 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 the 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 deployments. The interfaces that the firewall supports are:

- **Physical Interfaces**—The firewall has two kinds of Ethernet interfaces, co-axial 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, and tunnel interfaces. You must set up the physical interface before defining a VLAN or a tunnel interface.

Common Building Blocks for Firewall Interfaces

The following table describes the components of the **Network > Interfaces** page 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".

Table 61. Common Building Blocks for Firewall Interfaces

Field	Description
Interface (Interface Name)	The interface name is predefined and you cannot change it. You can append a numeric suffix for subinterfaces, aggregate interfaces, VLAN interfaces, loopback interfaces, and tunnel interfaces.
Interface Type	For Ethernet interfaces (**Network > Interfaces > Ethernet**), you can select the interface type: • Tap • HA • Decrypt Mirror (PA-7000 Series, PA-5000 Series, and PA-3000 Series firewalls only) • Virtual Wire • Layer 2 • Layer 3 • Log Card (PA-7000 Series firewall only) • Aggregate Ethernet
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.
Link State	For Ethernet interfaces, this column 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 an icon to display a tool tip that indicates the link speed and duplex settings of the interface.
IP Address	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 for the interface: static, Dynamic Host Configuration Protocol (DHCP), or Point-to-Point Protocol over Ethernet (PPPoE).
Virtual Router	Assign a virtual router to the interface, or click the **Virtual Router** link to define a new one (see "Configuring a Virtual Router"). Selecting **None** removes the current virtual router assignment from the interface.
Tag	Enter the VLAN tag (1-4094) for the subinterface.

Table 61. Common Building Blocks for Firewall Interfaces

Field	Description
VLAN	Select a VLAN, or click the **VLAN** link to define a new VLAN (see “Configuring VLAN Support”). Selecting **None** removes 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 the **Virtual System** link to define a new vsys.
Security Zone	Select a security zone for the interface, or click the **Zone** link to define a new zone. Selecting **None** removes the current zone assignment from the interface.
Features	For Ethernet interfaces, this column indicates whether the following features are enabled: Link Aggregation Control Protocol (LACP) QoS Quality of Service (QoS) profile Link Layer Discovery Protocol (LLDP) NetFlow profile IP Dynamic Host Configuration Protocol (DHCP) client—The interface acts as a DHCP client and receives a dynamically assigned IP address.
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 the **Add Interface** button to create an interface or click the name of an existing interface (ethernet1/1, for example) to edit it.

On PA-7000 Series firewalls, you must “Configure a Log Card Interface” for one data port.

Table 62. Common Building Blocks for PA-7000 Series Firewall Interfaces

Field	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 platform, select **Slot 1**.
Interface (Interface Name)	Select the name of an interface that is associated with the selected **Slot**.

Configure a Layer 2 Interface

▶ *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.

Table 63. Layer 2 Interface Settings

Field	Configured In	Description
Interface Name	**Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment	**Ethernet Interface**	Enter an optional description for the interface.
Interface Type	**Ethernet Interface**	Select **Layer2**.
Netflow Profile	**Ethernet Interface**	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click the **Netflow Profile** link to define a new profile (see "Configuring Netflow Settings"). Selecting **None** removes the current NetFlow server assignment from the interface. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don't support this feature.*
VLAN	**Ethernet Interface > Config**	To enable switching between Layer 2 interfaces or to enable routing through a VLAN interface, select a VLAN or click the **VLAN** link to define a new VLAN (see "Configuring VLAN Support"). Selecting **None** removes the current VLAN 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 the **Virtual System** link to define a new vsys.
Security Zone	**Ethernet Interface > Config**	Select a security zone for the interface or click the **Zone** link to define a new zone. Selecting **None** removes 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	**Ethernet Interface > Advanced**	Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State	**Ethernet Interface > Advanced**	Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).
Enable LLDP	**Ethernet Interface > Advanced > LLDP**	Select this option to enable Link Layer Discovery Protocol (LLDP) on the interface. LLDP functions at the link layer to discover neighboring devices and their capabilities.
Profile	**Ethernet Interface > Advanced > LLDP**	If LLDP is enabled, select an LLDP profile to assign to the interface or click the **LLDP Profile** link to create a new profile (see "Defining LLDP Profiles"). Selecting **None** causes the firewall to use global defaults.

Configure a 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 Layer 2 subinterface, "Configure a Layer 2 Interface", select the row of that physical Interface, click **Add Subinterface**, and specify the following information.

Table 64. Layer 2 Subinterface Settings

Field	Description
Interface Name	The read-only **Interface Name** field displays the name of the physical interface you selected. In the adjacent field, enter a numeric suffix (1-9999) to identify the subinterface.
Comment	Enter an optional description for the subinterface.
Tag	Enter the VLAN tag (1-4094) 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 the **Netflow Profile** link to define a new profile (see "Configuring Netflow Settings"). Selecting **None** removes the current NetFlow server assignment from the subinterface. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don't support this feature.*
VLAN	To enable switching between Layer 2 interfaces or to enable routing through a VLAN interface, select a VLAN, or click the **VLAN** link to define a new VLAN (see "Configuring VLAN Support"). Selecting **None** removes 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 the **Virtual System** link to define a new vsys.
Security Zone	Select a security zone for the subinterface or click the **Zone** link to define a new zone. Selecting **None** removes the current zone assignment from the subinterface.

Configure a Layer 3 Interface

▶ *Network > Interfaces > Ethernet*

To configure a Layer 3 interface, click the name of an Interface (ethernet1/1, for example) that is not configured and specify the following information.

Table 65. Layer 3 Interface Settings

Field	Configured In	Description
Interface Name	**Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment	**Ethernet Interface**	Enter an optional description for the interface.
Interface Type	**Ethernet Interface**	Select **Layer3**.

Table 65. Layer 3 Interface Settings

Field	Configured In	Description
Netflow Profile	**Ethernet Interface**	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click the **Netflow Profile** link to define a new profile (see "Configuring Netflow Settings"). Selecting **None** removes the current NetFlow server assignment from the interface. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don't support this feature.*
Virtual Router	**Ethernet Interface > Config**	Select a virtual router, or click the **Virtual Router** link to define a new one (see "Configuring a Virtual Router"). Selecting **None** removes the current virtual router 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 (vsys) for the interface or click the **Virtual System** link to define a new vsys.
Security Zone	**Ethernet Interface > Config**	Select a security zone for the interface or click the **Zone** link to define a new zone. Selecting **None** removes 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	**Ethernet Interface > Advanced**	Select whether the interface transmission mode is full-duplex (full), half-duplex (half), or negotiated automatically (auto).
Link State	**Ethernet Interface > Advanced**	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. Selecting **None** removes the current profile assignment from the interface.
MTU	**Ethernet Interface > Advanced > Other Info**	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9192, default 1500). 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	**Ethernet Interface > Advanced > Other Info**	Select this check box if you want to adjust the maximum segment size (MSS) to 40 bytes less than the interface MTU. This setting addresses situations where a tunnel through the network requires a smaller MSS. If a packet cannot fit within the MSS without fragmenting, this setting enables the adjustment.

Table 65. Layer 3 Interface Settings

Field	Configured In	Description
Untagged Subinterface	**Ethernet Interface > Advanced > Other Info**	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 [media access control (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 this check box 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 the Enable NDP Proxy check box is checked, you can filter numerous Address entries by entering a search string and clicking the Apply Filter icon ➡.
Address	**Ethernet Interface > Advanced > NDP Proxy**	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 the **Negate** check box to instruct the firewall not to respond to these IP addresses.
Negate	**Ethernet Interface > Advanced > NDP Proxy**	Select the **Negate** check box 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.
Profile	**Ethernet Interface > Advanced > LLDP**	If LLDP is enabled, select an LLDP profile to assign to the interface or click the **LLDP Profile** link to create a new profile (see "Defining LLDP Profiles"). Selecting **None** causes the firewall to use global defaults.

Table 65. Layer 3 Interface Settings

Field	Configured In	Description
For an IPv4 address		
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. **Note:** *Firewalls that are in active/active high availability (HA) mode do not support PPPoE or DHCP Client.* Based on your IP address method selection, the options displayed in the tab will vary.
• 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 for IPv4 or 2001:db8::/32 for IPv6). • Select an existing address object of type **IP netmask**. • Click the **Address** link 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**.
• IPv4 address **Type** = **PPPoE**		
Enable	**Ethernet Interface > IPv4 > PPPoE > General**	Select this check box to activate the interface for PPPoE termination.
Username	**Ethernet Interface > IPv4 > PPPoE > General**	Enter the user name for the point-to-point connection.
Password/Confirm Password	**Ethernet Interface > IPv4 > PPPoE > General**	Enter and then confirm the password for the user name.
Show PPPoE Client Runtime Info	**Ethernet Interface > IPv4 > PPPoE > General**	Optionally, click this link to open 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). Selecting **None** removes the current protocol assignment from the interface.

Table 65. Layer 3 Interface Settings

Field	Configured In	Description
Static Address	**Ethernet Interface > IPv4 > PPPoE > Advanced**	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 for IPv4 or 2001:db8::/32 for IPv6). • Select an existing address object of type **IP netmask**. • Click the **Address** link 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	**Ethernet Interface > IPv4 > PPPoE > Advanced**	Select this check box to automatically create a default route that points to the PPPoE peer when connected.
Default Route Metric	**Ethernet Interface > IPv4 > PPPoE > Advanced**	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 (optional, range 1-65535). The priority level increases as the numeric value decreases.
Access Concentrator	**Ethernet Interface > IPv4 > PPPoE > Advanced**	Optionally, enter the name of the access concentrator on the Internet service provider end to which the firewall connects (no default).
Service	**Ethernet Interface > IPv4 > PPPoE > Advanced**	Optionally, enter the service string (no default).
Passive	**Ethernet Interface > IPv4 > PPPoE > Advanced**	Select this check box 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 this check box to activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server	**Ethernet Interface > IPv4**	Select this check box to automatically create a default route that points to the default gateway that the DHCP server provides.
Default Route Metric	**Ethernet Interface > IPv4**	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 1-65535, no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info	**Ethernet Interface > IPv4**	Click this button 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).

Table 65. Layer 3 Interface Settings

Field	Configured In	Description
For an IPv6 address		
Enable IPv6 on the interface	**Ethernet Interface > IPv6**	Select this check box to enable IPv6 addressing on this interface.
Interface ID	**Ethernet 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	**Ethernet Interface > IPv6**	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 the **Address** link to create an address object. • **Enable address on interface**—Select this check box to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Select this check box to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select this check box to include routing through the nearest node. • **Send Router Advertisement**—Select this check box 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 only apply 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 2592000. – **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 604800. – **On-link**—Select this check box if systems that have addresses within the prefix are reachable without a router. – **Autonomous**—Select this check box if systems can independently create an IP address by combining the advertised prefix with an interface ID.
Enable Duplication Address Detection	**Ethernet Interface > IPv6**	Select this check box to enable duplicate address detection (DAD), then configure the other fields in this section.
DAD Attempts	**Ethernet Interface > IPv6**	Specify the number of DAD attempts within the neighbor solicitation interval (**NS Interval**) before the attempt to identify neighbors fails (range 1-10, default 1).
Reachable Time	**Ethernet Interface > IPv6**	Specify the length of time (in seconds) that a neighbor remains reachable after a successful query and response (range 1-36000, default 30).

Table 65. Layer 3 Interface Settings

Field	Configured In	Description
NS Interval (neighbor solicitation interval)	**Ethernet Interface > IPv6**	Specify the number of seconds for DAD attempts before failure is indicated (range 1-10, default 1).
Enable Router Advertisement	**Ethernet Interface > IPv6**	To provide stateless address auto-configuration (SLAAC) on IPv6 interfaces, select this check box and configure the other fields in this section. 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 option 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 (for details, see “Address” in this table). If you set RA options for any IP address, you must select the **Enable Router Advertisement** option for the interface.
Min Interval (sec)	**Ethernet Interface > IPv6**	Specify the minimum interval (in seconds) between RAs that the firewall will send (range 3-1350, default 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)	**Ethernet Interface > IPv6**	Specify the maximum interval (in seconds) between RAs that the firewall will send (range 4-1800, default 600). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit	**Ethernet Interface > IPv6**	Specify the hop limit to apply to clients for outgoing packets (range 1-255, default 64). Enter 0 for no hop limit.
Link MTU	**Ethernet Interface > IPv6**	Specify the link maximum transmission unit (MTU) to apply to clients. Select **unspecified** for no link MTU (range 1280-9192, default unspecified).
Reachable Time (ms)	**Ethernet Interface > IPv6**	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 0-3600000, default unspecified).
Retrans Time (ms)	**Ethernet Interface > IPv6**	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 0-4294967295, default unspecified).
Router Lifetime (sec)	**Ethernet Interface > IPv6**	Specify how long (in seconds) the client will use the firewall as the default gateway (range 0-9000, default 1800). 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	**Ethernet Interface > IPv6**	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.

Table 65. Layer 3 Interface Settings

Field	Configured In	Description
Managed Configuration	**Ethernet Interface > IPv6**	Select this check box to indicate to the client that addresses are available via DHCPv6.
Other Configuration	**Ethernet Interface > IPv6**	Select this check box to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check	**Ethernet Interface > IPv6**	Select this check box 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.

Configure a 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 Layer 3 subinterface, "Configure a Layer 3 Interface", select the row of that physical Interface, click **Add Subinterface**, and specify the following information.

Table 66. Layer 3 Subinterface Settings

Field	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 (1-9999) to identify the subinterface.
Comment	**Layer3 Subinterface**	Enter an optional description for the subinterface.
Tag	**Layer3 Subinterface**	Enter the VLAN tag (1-4094) for the subinterface.
Netflow Profile	**Layer3 Subinterface**	If you want to export unidirectional IP traffic that traverses an ingress subinterface to a NetFlow server, select the server profile or click the **Netflow Profile** link to define a new profile (see "Configuring Netflow Settings"). Selecting **None** removes the current NetFlow server assignment from the subinterface. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don't support this feature.*
Virtual Router	**Layer3 Subinterface > Config**	Assign a virtual router to the interface, or click the **Virtual Router** link to define a new one (see "Configuring a Virtual Router"). Selecting **None** removes the current virtual router assignment from the interface.
Virtual System	**Layer3 Subinterface > Config**	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the subinterface or click the **Virtual System** link to define a new vsys.
Security Zone	**Layer3 Subinterface > Config**	Select a security zone for the subinterface, or click the **Zone** link to define a new zone. Selecting **None** removes the current zone assignment from the subinterface.
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. Selecting **None** removes the current profile assignment from the interface.
MTU	**Layer3 Subinterface > Advanced > Other Info**	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9192, default 1500). 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.

Table 66. Layer 3 Subinterface Settings (Continued)

Field	Configured In	Description
Adjust TCP MSS	**Layer3 Subinterface > Advanced > Other Info**	Select this check box if you want to adjust the maximum segment size (MSS) to 40 bytes less than the interface MTU. This setting addresses situations where a tunnel through the network requires a smaller MSS. If a packet cannot fit within the MSS without fragmenting, this setting enables the adjustment.
IP Address MAC Address	**Layer3 Subinterface > 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 [media access control (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	**Layer3 Subinterface > 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	**Layer3 Subinterface > Advanced > NDP Proxy**	Click 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 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 the **Enable NDP Proxy** check box is selected, you can filter numerous **Address** entries by entering a filter and clicking on the Apply Filter icon (the gray arrow).
Address	**Layer3 Subinterface > Advanced > NDP Proxy**	Click **Add** to enter 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 the **Negate** check box to instruct the firewall not to respond to these IP addresses.
Negate	**Layer3 Subinterface > Advanced > NDP Proxy**	Select the **Negate** check box for an address to prevent NDP proxy for that address. You can negate a subset of the specified IP address range or IP subnet.
For an IPv4 address		
Type	**Layer3 Subinterface > IPv4**	Select the method for assigning an IPv4 address type to the subinterface: • **Static**—You must manually specify the IP address. • **DHCP Client**—Enables the subinterface to act as a Dynamic Host Configuration Protocol (DHCP) client and receive a dynamically assigned IP address. **Note:** *Firewalls that are in active/active high availability (HA) mode don't support DHCP Client.* Based on your IP address method selection, the options displayed in the tab will vary.

Table 66. Layer 3 Subinterface Settings (Continued)

Field	Configured In	Description
• IPv4 address **Type** = **Static**		
IP	**Layer3 Subinterface > 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 for IPv4 or 2001:db8::/32 for IPv6). • Select an existing address object of type **IP netmask**. • Click the **Address** link 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**.
• IPv4 address **Type** = **DHCP**		
Enable	**Layer3 Subinterface > IPv4**	Select this check box to activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server	**Layer3 Subinterface > IPv4**	Select this check box to automatically create a default route that points to the default gateway that the DHCP server provides.
Default Route Metric	**Layer3 Subinterface > IPv4**	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 1-65535, no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info	**Layer3 Subinterface > IPv4**	Click this button 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	**Layer3 Subinterface > IPv6**	Select this check box to enable IPv6 addressing on this interface.
Interface ID	**Layer3 Subinterface > 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.

Table 66. Layer 3 Subinterface Settings (Continued)

Field	Configured In	Description
Address	**Layer3 Subinterface > IPv6**	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 the **Address** link to create an address object. • **Enable address on interface**—Click to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Click to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Click to include routing through the nearest node. • **Send Router Advertisement**—Click 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 2592000. – **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 604800. – **On-link**—Click if systems that have addresses within the prefix are reachable without a router. – **Autonomous**—Click if systems can independently create an IP address by combining the advertised prefix with an interface ID.
Enable Duplication Address Detection	**Layer3 Subinterface > IPv6**	Select this check box to enable duplicate address detection (DAD), then configure the other fields in this section.
DAD Attempts	**Layer3 Subinterface > IPv6**	Specify the number of DAD attempts within the neighbor solicitation interval (**NS Interval**) before the attempt to identify neighbors fails (range 1-10, default 1).
Reachable Time	**Layer3 Subinterface > IPv6**	Specify the length of time (in seconds) that a neighbor remains reachable after a successful query and response (range 1-36000, default 30).
NS Interval (neighbor solicitation interval)	**Layer3 Subinterface > IPv6**	Specify the number of seconds for DAD attempts before failure is indicated (range 1-10, default 1).

Table 66. Layer 3 Subinterface Settings (Continued)

Field	Configured In	Description
Enable Router Advertisement	**Layer3 Subinterface > IPv6**	To provide stateless address auto-configuration (SLAAC) on IPv6 interfaces, select this check box and configure the other fields in this section. 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 option 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 (for details, see "Address" in this table). If you set RA options for any IP address, you must select the **Enable Router Advertisement** option for the interface.
Min Interval (sec)	**Layer3 Subinterface > IPv6**	Specify the minimum interval (in seconds) between RAs that the firewall will send (range 3-1350, default 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)	**Layer3 Subinterface > IPv6**	Specify the maximum interval (in seconds) between RAs that the firewall will send (range 4-1800, default 600). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit	**Layer3 Subinterface > IPv6**	Specify the hop limit to apply to clients for outgoing packets (range 1-255, default 64). Enter 0 for no hop limit.
Link MTU	**Layer3 Subinterface > IPv6**	Specify the link maximum transmission unit (MTU) to apply to clients. Select **unspecified** for no link MTU (range 1280-9192, default unspecified).
Reachable Time (ms)	**Layer3 Subinterface > IPv6**	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 0-3600000, default unspecified).
Retrans Time (ms)	**Layer3 Subinterface > IPv6**	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 0-4294967295, default unspecified).
Router Lifetime (sec)	**Layer3 Subinterface > IPv6**	Specify how long (in seconds) the client will use the firewall as the default gateway (range 0-9000, default 1800). 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	**Layer3 Subinterface > IPv6**	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	**Layer3 Subinterface > IPv6**	Select this check box to indicate to the client that addresses are available via DHCPv6.

Table 66. Layer 3 Subinterface Settings (Continued)

Field	Configured In	Description
Other Configuration	**Layer3 Subinterface > IPv6**	Select this check box to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check	**Layer3 Subinterface > IPv6**	Select this check box 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.

Configure a Virtual Wire Interface

▶ *Network > Interfaces > Ethernet*

A virtual wire interface binds two Ethernet ports together, allowing for all traffic to pass between the ports, or just traffic with selected VLAN tags (no other switching or routing services are available). You can also create Virtual Wire subinterfaces and classify traffic according to an IP address, IP range, or subnet. A virtual wire requires no changes to adjacent network devices.

To set up a virtual wire through the firewall, you must first define the virtual wire interfaces, as described in the following procedure, and then create the virtual wire using the interfaces that you created.

1. Identify the interface you want to use for the virtual wire on the **Ethernet** tab, and remove it from the current security zone, if any.
2. Click the interface name and specify the following information.

Table 67. Virtual Wire Interface Settings

Field	Configured In	Description
Interface Name	**Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment	**Ethernet Interface**	Enter an optional description for the interface.
Interface Type	**Ethernet Interface**	Select **Virtual Wire**.
Virtual Wire	**Ethernet Interface > Config**	Select a virtual wire, or click the **Virtual Wire** link to define a new one (see “Defining Virtual Wires”). Selecting **None** removes the current virtual wire 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 the **Virtual System** link to define a new vsys.
Security Zone	**Ethernet Interface > Config**	Select a security zone for the interface, or click the **Zone** link to define a new zone. Selecting **None** removes 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.

Table 67. Virtual Wire Interface Settings (Continued)

Field	Configured In	Description
Link Duplex	**Ethernet Interface > Advanced**	Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State	**Ethernet Interface > Advanced**	Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).
Enable LLDP	**Ethernet Interface > Advanced > LLDP**	Select this option to enable Link Layer Discovery Protocol (LLDP) on the interface. LLDP functions at the link layer to discover neighboring devices and their capabilities.
Profile	**Ethernet Interface > Advanced > LLDP**	If LLDP is enabled, select an LLDP profile to assign to the interface or click the **LLDP Profile** link to create a new profile (see “Defining LLDP Profiles”). Selecting **None** causes the firewall to use global defaults.

Configure a 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 vwire subinterface, "Configure a Virtual Wire Interface", select the row for that interface, click **Add Subinterface**, and specify the following information.

Table 68. Virtual Wire Subinterface Settings

Field	Description
Interface Name	The read-only **Interface Name** field displays the name of the vwire interface you selected. In the adjacent field, enter a numeric suffix (1-9999) to identify the subinterface.
Comment	Enter an optional description for the subinterface.
Tag	Enter the VLAN tag (0-4094) 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 the **Netflow Profile** link to define a new profile (see "Configuring Netflow Settings"). Selecting **None** removes the current NetFlow server assignment from the subinterface. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don't support this feature.*
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 the **Virtual Wire** link to define a new one (see "Defining Virtual Wires"). Selecting **None** removes 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 the **Virtual System** link to define a new vsys.
Security Zone	Select a security zone for the subinterface, or click the **Zone** link to define a new zone. Selecting **None** removes the current zone assignment from the subinterface.

Configure a 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.

Table 69. Tap Interface Settings

Field	Configured In	Description
Interface Name	**Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment	**Ethernet Interface**	Enter an optional description for the interface.
Interface Type	**Ethernet Interface**	Select **Tap**.

Table 69. Tap Interface Settings (Continued)

Field	Configured In	Description
Netflow Profile	**Ethernet Interface**	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click the **Netflow Profile** link to define a new profile (see "Configuring Netflow Settings"). Selecting **None** removes the current NetFlow server assignment from the interface. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don't support this feature.*
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 the **Virtual System** link to define a new vsys.
Security Zone	**Ethernet Interface > Config**	Select a security zone for the interface or click the **Zone** link to define a new zone. Selecting **None** removes 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	**Ethernet Interface > Advanced**	Select whether the interface transmission mode is full-duplex (**full**), half-duplex (**half**), or negotiated automatically (**auto**).
Link State	**Ethernet Interface > Advanced**	Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically (**auto**).

Configure a Log Card Interface

▶ *Network > Interfaces > Ethernet*

On PA-7000 Series firewalls, one data port must have an interface type of **Log Card**. This is because the traffic and logging capabilities of this platform exceed the capabilities of the management port. A log card data port performs log forwarding for syslog, email, Simple Network Management Protocol (SNMP), and WildFire™ file-forwarding. Only one port on the firewall can be a log card interface. If you enable log forwarding but do not configure any interface as the log card, a commit error occurs.

To configure a log card interface, click the name of an Interface (ethernet1/16, for example) that is not configured and specify the following information.

Table 70. Log Card Interface Settings

Field	Configured In	Description
Slot	**Ethernet Interface**	Select the slot number (1-12) of the interface.
Interface Name	**Ethernet Interface**	The interface name is predefined and you cannot change it.
Comment	**Ethernet Interface**	Enter an optional description for the interface.
Interface Type	**Ethernet Interface**	Select **Log Card**.

Table 70. Log Card Interface Settings (Continued)

Field	Configured In	Description
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	**Ethernet Interface > Log Card Forwarding**	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	**Ethernet Interface > Advanced**	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	**Ethernet Interface > Advanced**	Select whether the interface status is enabled (**up**), disabled (**down**), or determined automatically based on the connection (**auto**). The default is **auto**.

Configure a Log Card Subinterface

▶ *Network > Interfaces > Ethernet*

To add a log card subinterface, “Configure a Log Card Interface”, select the row for that interface, click **Add Subinterface**, and specify the following information.

Table 71. Log Card Subinterface Settings

Field	Configured In	Description
Interface Name	**LPC Subinterface**	The read-only **Interface Name** field displays the name of the log card interface you selected. In the adjacent field, enter a numeric suffix (1-9999) to identify the subinterface.
Comment	**LPC Subinterface**	Enter an optional description for the interface.
Tag	**LPC Subinterface**	Enter the VLAN tag (0-4094) for the subinterface. It is a best practice to 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 the **Virtual Systems** link 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.

Table 71. Log Card Subinterface Settings (Continued)

Field	Configured In	Description
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	**Ethernet Interface > Log Card Forwarding**	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.

Configure a 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. Decryption port mirroring is only available on PA-7000 Series firewalls, PA-5000 Series firewalls, and PA-3000 Series firewalls. To enable the feature, you must acquire and install the free license.

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.

Table 72. Decrypt Mirror Interface Settings

Field	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**).

Configure an Aggregate Interface Group

▶ *Network > Interfaces > Ethernet*

An aggregate interface group combines multiple Ethernet interfaces using IEEE 802.1AX link aggregation. You can aggregate 1Gbps or 10Gbps XFP and SFP+ Ethernet. The aggregate interface you create becomes a logical interface. The following are properties of the logical interface, not the underlying physical interfaces: configuration assignments (virtual system, virtual router, virtual wire, VLAN, security zone), IP addresses, management profile, Link Aggregation Control Protocol (LACP) configuration, Address Resolution Protocol (ARP) entries, and Neighbor Discovery (ND) entries. Therefore, after creating the group, perform operations such as configuring Layer 2 or Layer 3 parameters on the aggregate group, not on individual interfaces.

The following rules apply to aggregate groups:

- Within a group, the 1 Gbps links must be all copper or all fiber.
- A group can have up to eight interfaces.
- Aggregate groups support HA, virtual wire, Layer 2, or Layer 3 interfaces. Within a group, all the interfaces must be the same type. PAN-OS validates this during the commit operation.
- You can use aggregate groups for redundancy and throughput scaling on the HA3 (packet forwarding) link in active/active high availability (HA) deployments. Support for HA3 is limited to the PA-500, PA-3000 Series, PA-4000 Series, and PA-5000 Series firewalls.
- If you enable LACP for an aggregate group, support is limited to HA3, Layer 2, and Layer 3 interfaces. You cannot enable LACP for virtual wire interfaces. Support for LACP-enabled groups is limited to the PA-500, PA-3000 Series, PA-4000 Series, PA-5000 Series, and PA-7000 Series firewalls.

To configure an aggregate group, click **Add Aggregate Group**, configure the settings in the following table, then assign interfaces to the group as described in "Configure an Aggregate Interface".

Table 73. Aggregate Interface Group Settings

Field	Configured In	Description
Interface Name	**Aggregate Ethernet Interface**	The read-only **Interface Name** field is set to **ae**. In the adjacent field, enter a numeric suffix (1-8) to identify the aggregate group.
Comment	**Aggregate Ethernet Interface**	Enter an optional description for the interface.
Interface Type	**Aggregate Ethernet Interface**	Select the interface type, which controls the remaining configuration requirements and options: • **HA**—Only select this option if the interface is an HA3 link between two firewalls in an active/active deployment. Optionally select a **Netflow Profile** and configure the **LACP** tab as described below. • **Virtual Wire**—Optionally select a **Netflow Profile**, and configure the **Config** and **Advanced** tabs as described in Table 67. • **Layer 2**—Optionally select a **Netflow Profile**; configure the **Config** and **Advanced** tabs as described in Table 63; and optionally configure the **LACP** tab as described below. • **Layer 3**—Optionally select a **Netflow Profile**; configure the **Config**, **IPv4** or **IPv6**, and **Advanced** tabs as described in Table 65; and optionally configure the **LACP** tab as described below.

Table 73. Aggregate Interface Group Settings (Continued)

Field	Configured In	Description
Netflow Profile	**Aggregate Ethernet Interface**	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click the **Netflow Profile** link to define a new profile (see "Configuring Netflow Settings"). Selecting **None** removes the current NetFlow server assignment from the aggregate interface group. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don't support this feature.*
Enable LACP	**Aggregate Ethernet Interface > LACP**	Select this check box if you want to enable Link Aggregation Control Protocol (LACP) for the aggregate group. LACP is disabled by default.
Mode	**Aggregate Ethernet Interface > LACP**	Select the LACP mode of the firewall. Between any two LACP peers, it is recommended that one be active and the other passive. LACP cannot function if both peers are passive. • **Active**—The firewall actively queries the LACP status (available or unresponsive) of peer devices. • **Passive** (default)—The firewall passively responds to LACP status queries from peer devices.
Transmission Rate	**Aggregate Ethernet Interface > LACP**	Select the rate at which the firewall exchanges queries and responses with peer devices: • **Fast**—Every second • **Slow**—Every 30 seconds (this is the default setting)
Fast Failover	**Aggregate Ethernet Interface > LACP**	Select this check box 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**	The number that determines whether the firewall or its peer overrides the other with respect to port priorities (see the **Max Ports** field description below). Note that the lower the number, the higher the priority. The range is 1-65535 and the default is 32768.
Max Ports	**Aggregate Ethernet Interface > LACP**	The number of interfaces (1-8) that can be active at any given time in an LACP aggregate group. The 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 port priorities of the interfaces to determine which are in standby mode. You set port priorities when configuring individual interfaces for the group.

Table 73. Aggregate Interface Group Settings (Continued)

Field	Configured In	Description
Same System MAC Address for Active-Passive HA	**Aggregate Ethernet Interface > LACP**	Firewalls in a high availability (HA) pair 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 is a best practice to minimize latency during failover. When the LACP peers are not virtualized, using the unique MAC address of each firewall is the best practice to minimize failover latency. If the firewalls are not in active/passive HA mode, PAN-OS ignores this field. (Firewalls in an active/active deployment require unique MAC addresses so PAN-OS automatically assigns them.) 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**	If you enabled **Use Same System MAC Address**, select a system-generated MAC address, or enter your own, for both firewalls in the HA pair. You must verify the address is globally unique.

Configure an Aggregate Interface

▶ *Network > Interfaces > Ethernet*

To configure an aggregate Ethernet interface, "Configure an Aggregate Interface Group" and click the name of the Interface you will assign to that aggregate group. The interface you select must be the same type as that defined for the aggregate group (for example, Layer3), though you will change the type to **Aggregate Ethernet** when you configure it. Specify the following information for the interface.

*If you enabled Link Aggregation Control Protocol (LACP) for the aggregate group, it is a best practice to 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.*

Table 74. Aggregate Ethernet Interface Settings

Field	Description
Interface Name	The interface name is predefined and you cannot change it.
Comment	Enter an optional description for the interface.
Interface Type	Select **Aggregate Ethernet**.
Aggregate Group	Assign the interface to an aggregate group.
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. An aggregate group might have more interfaces than it supports in active states. (In the aggregate group configuration, the **Max Ports** parameter determines the number of active interfaces). In this case, the port priority assigned to each interface determines whether it is active or standby. The lower the numeric value, the higher the priority. The range is 1-65535 and the default is 32768.

Configure an 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 "Enabling HA on the Firewall".

To configure an HA interface, click the name of an Interface (ethernet1/1, for example) that is not configured and specify the following information.

Table 75. HA Interface Settings

Field	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**).

Configure a VLAN Interface

▶ *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 “Configure a Layer 2 Interface”) to a VLAN interface.

Table 76. VLAN Interface Settings

Field	Configure In	Description
Interface Name	**VLAN Interface**	The read-only **Interface Name** field is set to `vlan`. In the adjacent field, enter a numeric suffix (1-9999) to identify the interface.
Comment	**VLAN Interface**	Enter an optional description for the interface.
Netflow Profile	**VLAN Interface**	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click the **Netflow Profile** link to define a new profile (see “Configuring Netflow Settings”). Selecting **None** removes the current NetFlow server assignment from the interface. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don’t support this feature.*
VLAN	**VLAN Interface > Config**	Select a VLAN or click the **VLAN** link to define a new one (see “Configuring VLAN Support”). Selecting **None** removes the current VLAN assignment from the interface.
Virtual Router	**VLAN Interface > Config**	Assign a virtual router to the interface, or click the **Virtual Router** link to define a new one (see “Configuring a Virtual Router”). Selecting **None** removes the current virtual router assignment from the interface.
Virtual System	**VLAN Interface > Config**	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click the **Virtual System** link to define a new vsys.
Security Zone	**VLAN Interface > Config**	Select a security zone for the interface, or click the **Zone** link to define a new zone. Selecting **None** removes the current zone assignment from the interface.

Table 76. VLAN Interface Settings (Continued)

Field	Configure In	Description
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. Selecting **None** removes the current profile assignment from the interface.
MTU	**VLAN Interface > Advanced > Other Info**	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9192, default 1500). 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	**VLAN Interface > Advanced > Other Info**	Select this check box if you want to adjust the maximum segment size (MSS) to 40 bytes less than the interface MTU. This setting addresses situations where a tunnel through the network requires a smaller MSS. If a packet cannot fit within the MSS without fragmenting, this setting enables the adjustment.
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.” It is recommended that you enable NDP Proxy if you are using Network Prefix Translation IPv6 (NPTv6). If the **Enable NDP Proxy** check box is selected, you can filter numerous **Address** entries by entering a filter and clicking on the Apply Filter icon (the green arrow).
Address	**VLAN Interface > Advanced > NDP Proxy**	Click **Add** to enter 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 the Negate check box, to instruct the firewall not to respond to these IP addresses.
Negate	**VLAN Interface > Advanced > NDP Proxy**	Select the **Negate** check box for an address to prevent NDP proxy for that address. You can negate a subset of the specified IP address range or IP subnet.

Table 76. VLAN Interface Settings (Continued)

Field	Configure In	Description
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. **Note:** *Firewalls that are in active/active high availability (HA) mode 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 for IPv4 or 2001:db8::/32 for IPv6). • Select an existing address object of type **IP netmask**. • Click the **Address** link 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**.
• IPv4 address **Type** = **DHCP**		
Enable	**VLAN Interface > IPv4**	Select this check box to activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server	**VLAN Interface > IPv4**	Select this check box to automatically create a default route that points to the default gateway that the DHCP server provides.
Default Route Metric	**VLAN Interface > IPv4**	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 1-65535, no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info	**VLAN Interface > IPv4**	Click this button 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 this check box to enable IPv6 addressing on this interface.

Table 76. VLAN Interface Settings (Continued)

Field	Configure In	Description
Interface ID	**VLAN 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	**VLAN Interface > IPv6**	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 the **Address** link to create an address object. • **Enable address on interface**—Select this check box to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Select this check box to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select this check box to include routing through the nearest node. • **Send RA**—Select this check box 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 only apply 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 2592000. – **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 604800. – **On-link**—Select this check box if systems that have addresses within the prefix are reachable without a router. – **Autonomous**—Select this check box if systems can independently create an IP address by combining the advertised prefix with an interface ID.
Enable Duplication Address Detection	**VLAN Interface > IPv6**	Select this check box to enable duplicate address detection (DAD), then configure the other fields in this section.
DAD Attempts	**VLAN Interface > IPv6**	Specify the number of DAD attempts within the neighbor solicitation interval (**NS Interval**) before the attempt to identify neighbors fails (range 1-10, default 1).
Reachable Time	**VLAN Interface > IPv6**	Specify the length of time (in seconds) that a neighbor remains reachable after a successful query and response (range 1-36000, default 30).
NS Interval (neighbor solicitation interval)	**VLAN Interface > IPv6**	Specify the number of seconds for DAD attempts before failure is indicated (range 1-10, default 1).

Table 76. VLAN Interface Settings (Continued)

Field	Configure In	Description
Enable Router Advertisement	**VLAN Interface > IPv6**	To provide stateless address auto-configuration (SLAAC) on IPv6 interfaces, select this check box and configure the other fields in this section. 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 option 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 (for details, see "Address" in this table). If you set RA options for any IP address, you must select the **Enable Router Advertisement** option for the interface.
Min Interval (sec)	**VLAN Interface > IPv6**	Specify the minimum interval (in seconds) between RAs that the firewall will send (range 3-1350, default 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)	**VLAN Interface > IPv6**	Specify the maximum interval (in seconds) between RAs that the firewall will send (range 4-1800, default 600). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit	**VLAN Interface > IPv6**	Specify the hop limit to apply to clients for outgoing packets (range 1-255, default 64). Enter 0 for no hop limit.
Link MTU	**VLAN Interface > IPv6**	Specify the link maximum transmission unit (MTU) to apply to clients. Select **unspecified** for no link MTU (range 1280-9192, default unspecified).
Reachable Time (ms)	**VLAN Interface > IPv6**	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 0-3600000, default unspecified).
Retrans Time (ms)	**VLAN Interface > IPv6**	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 0-4294967295, default unspecified).
Router Lifetime (sec)	**VLAN Interface > IPv6**	Specify how long (in seconds) the client will use the firewall as the default gateway (range 0-9000, default 1800). 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	**VLAN Interface > IPv6**	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	**VLAN Interface > IPv6**	Select this check box to indicate to the client that addresses are available via DHCPv6.
Other Configuration	**VLAN Interface > IPv6**	Select this check box to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check	**VLAN Interface > IPv6**	Select this check box 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.

Configure a Loopback Interface

▶ *Network > Interfaces > Loopback*

Table 77. Loopback Interface Settings

Field	Configure In	Description
Interface Name	**Loopback Interface**	The read-only **Interface Name** field is set to `loopback`. In the adjacent field, enter a numeric suffix (1-9999) to identify the interface.
Comment	**Loopback Interface**	Enter an optional description for the interface.
Netflow Profile	**Loopback Interface**	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click the **Netflow Profile** link to define a new profile (see "Configuring Netflow Settings"). Selecting **None** removes the current NetFlow server assignment from the interface. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don't support this feature.*
Virtual Router	**Loopback Interface > Config**	Assign a virtual router to the interface, or click the **Virtual Router** link to define a new one (see "Configuring a Virtual Router"). Selecting **None** removes the current virtual router assignment from the interface.
Virtual System	**Loopback Interface > Config**	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click the **Virtual System** link to define a new vsys.
Security Zone	**Loopback Interface > Config**	Select a security zone for the interface, or click the **Zone** link to define a new zone. Selecting **None** removes 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. Selecting **None** removes the current profile assignment from the interface.
MTU	**Tunnel Interface > Advanced > Other Info**	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9192, default 1500). 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	**Tunnel Interface > Advanced > Other Info**	Select this check box if you want to adjust the maximum segment size (MSS) to 40 bytes less than the interface MTU. This setting addresses situations where a tunnel through the network requires a smaller MSS. If a packet cannot fit within the MSS without fragmenting, this setting enables the adjustment.

Table 77. Loopback Interface Settings (Continued)

Field	Configure In	Description
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. • Type the entry 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). • Select an existing address object of type **IP netmask**. • Click the **Address** link 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 this check box to enable IPv6 addressing on this interface.
Interface ID	**Loopback 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	**Loopback Interface > IPv6**	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 the **Address** link to create an address object. • **Enable address on interface**—Select this check box to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Select this check box to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select this check box to include routing through the nearest node.

Configure a Tunnel Interface

▶ *Network > Interfaces > Tunnel*

Table 78. Tunnel Interface Settings

Field	Configure In	Description
Interface Name	**Tunnel Interface**	The read-only **Interface Name** field is set to `tunnel`. In the adjacent field, enter a numeric suffix (1-9999) to identify the interface.
Comment	**Tunnel Interface**	Enter an optional description for the interface.

Table 78. Tunnel Interface Settings (Continued)

Field	Configure In	Description
Netflow Profile	**Tunnel Interface**	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click the **Netflow Profile** link to define a new profile (see "Configuring Netflow Settings"). Selecting **None** removes the current NetFlow server assignment from the interface. **Note:** *The PA-4000 Series and PA-7000 Series firewalls don't support this feature.*
Virtual Router	**Tunnel Interface > Config**	Assign a virtual router to the interface, or click the **Virtual Router** link to define a new one (see "Configuring a Virtual Router"). Selecting **None** removes the current virtual router assignment from the interface.
Virtual System	**Tunnel Interface > Config**	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click the **Virtual System** link to define a new vsys.
Security Zone	**Tunnel Interface > Config**	Select a security zone for the interface, or click the **Zone** link to define a new zone. Selecting **None** removes 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. Selecting **None** removes the current profile assignment from the interface.
MTU	**Tunnel Interface > Advanced > Other Info**	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9192, default 1500). 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 for IPv4 or 2001:db8::/32 for IPv6). • Select an existing address object of type **IP netmask**. • Click the **Address** link 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	**Tunnel Interface > IPv6**	Select this check box 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.

Table 78. Tunnel Interface Settings (Continued)

Field	Configure In	Description
Address	**Tunnel Interface > IPv6**	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 the **Address** link to create an address object. • **Enable address on interface**—Select this check box to enable the IPv6 address on the interface. • **Use interface ID as host portion**—Select this check box to use the **Interface ID** as the host portion of the IPv6 address. • **Anycast**—Select this check box to include routing through the nearest node.

Configuring a Virtual Router

▶ *Network > Virtual Routers*

Use this page to define Virtual Routers. Defining virtual routers allows you to set up forwarding rules for Layer 3 and enable the use of dynamic routing protocols. Each Layer 3 interface, loopback interface, and VLAN interface defined on the firewall should be associated with a virtual router. Each interface can belong to only one virtual router.

Defining a Virtual Router requires assignment configuration of the settings on the **Router Settings > General** tab and any of the following tabs as required by your network topology:

- **Static Routes** tab: See “Configuring the Static Routes tab”.
- **Redistribution Profile** tab: See “Configuring the Redistribution Profiles Tab”.
- **RIP** tab: See “Configuring the RIP Tab”.
- **OSPF** tab: See “Configuring the OSPF Tab”.
- **OSPFv3** tab: See “Configuring the OSPFv3 Tab”.
- **BGP** tab: See “Configuring the BGP Tab”.
- **Multicast** tab: See “Configuring the Multicast Tab”.
- **ECMP** tab: See “Building Blocks of ECMP”.

After you have configured a portion of a Virtual Router, from the Network > Virtual Routers page, you can see information for a particular virtual router by clicking on More Runtime Stats in the last column.

- **More Runtime Stats** link: See “More Runtime Stats for a Virtual Router”.

Configuring the General tab

▶ *Network > Virtual Router > Router Settings > General*

All Virtual Router configurations require that you assign Layer 3 interfaces and administrative distance metrics as described in the following table:

Table 79. Virtual Router Settings - General Tab

Field	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. When you select an interface, it is included in the virtual router and can be used as an outgoing interface in the virtual router's routing tab. To specify the interface type, refer to "Configuring a Firewall Interface". *When you add an interface, its connected routes are added automatically.*
Administrative Distances	Specify the following administrative distances: • Static routes (10-240, default 10). • OSPF Int (10-240, default 30). • OSPF Ext (10-240, default 110). • IBGP (10-240, default 200). • EBGP (10-240, default 20). • RIP (10-240, default 120).

Configuring the Static Routes tab

▶ *Network > Virtual Router > Static Routes*

Optionally enter one or more static routes. Click the **IP** or **IPv6** tab to specify the route using IPv4 or IPv6 addresses. 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.

Table 80. Virtual Router Settings - Static Routes Tab

Field	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).
Interface	Select the interface to forward packets to the destination, or configure the next hop settings, or both.
Next Hop	Specify the following next hop settings: • **None**—Select if there is no next hop for the route. • **IP Address**—Specify the IP address of the next hop router. • **Discard**—Select if you want to drop traffic that is addressed to this destination. • **Next VR**—Select a virtual router in the firewall as the next hop. This option allows you to route internally between virtual routers within a single firewall.
Admin Distance	Specify the administrative distance for the static route (10-240, default 10).

Table 80. Virtual Router Settings - Static Routes Tab (Continued)

Field	Description
Metric	Specify a valid metric for the static route (1 - 65535).
No Install	Select if you do not want to install the route in the forwarding table. The route is retained in the configuration for future reference.

Configuring the Redistribution Profiles Tab

▶ *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.

Table 81. Virtual Router Settings - Redistribution Profiles Tab

Field	Description
Name	Click **Add** to display the **Redistribution Profile** page, and enter the profile name.
Priority	Enter a priority (range 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 check boxes to specify 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 the icon associated with the entry.
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 the icon associated with the entry.
OSPF Filter Tab	
Path Type	Select check boxes to specify the route types of the candidate OSPF route.

Table 81. Virtual Router Settings - Redistribution Profiles Tab (Continued)

Field	Description
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 the ⊟ icon associated with the entry.
Tag	Specify OSPF tag values. Enter a numeric tag value (1-255), and click Add. To remove an entry, click the ⊟ icon associated with the entry.
BGP Filter Tab	
Community	Specify a community for BGP routing policy.
Extended Community	Specify an extended community for BGP routing policy.

Configuring the RIP Tab

▶ *Network > Virtual Router > RIP*

Configuring the Routing Information Protocol (RIP) requires configuring the following general settings:

Table 82. Virtual Router Settings - RIP Tab

Field	Description
Enable	Select the check box to enable the RIP protocol.
Reject Default Route	Select the check box if you do not want to learn any default routes through RIP. Selecting the check box is highly recommended.

In addition, settings on the following tabs must be configured:

- **Interfaces** tab: See “Configuring the Interfaces Tab”.
- **Timers** tab: See “Configuring the Timers Tab”.
- **Auth Profiles** tab: See “Configuring the Auth Profiles Tab”.
- **Export Rules** tab: See “Configuring the Export Rules Tab”.

Configuring the Interfaces Tab

▶ *Network > Virtual Router > RIP > Interfaces*

The following table describes the settings for the **Interfaces** tab.

Table 83. RIP Settings – Interfaces Tab

Field	Description
Interfaces	
Interface	Select the interface that runs the RIP protocol.
Enable	Select to enable these settings.
Advertise	Select to advertise a default route to RIP peers with the specified metric value.

Table 83. RIP Settings – Interfaces Tab (Continued)

Field	Description
Metric	Specify a metric value for the router advertisement. This field is visible only if the **Advertise** check box is selected.
Auth Profile	Select the profile.
Mode	Select **normal**, **passive**, or **send-only**.

Configuring the Timers Tab

▶ *Network > Virtual Router > RIP > Timers*

The following table describes the settings for the **Timers** tab.

Table 84. RIP Settings – Timers Tab

Field	Description
Timers	
Interval Seconds (sec)	Define the length of the timer interval in seconds. This duration is used for the remaining RIP timing fields (1 - 60).
Update Intervals	Enter the number of intervals between route update announcements (1 - 3600).
Expire Intervals	Enter the number of intervals between the time that the route was last updated to its expiration (1- 3600).
Delete Intervals	Enter the number of intervals between the time that the route expires to its deletion (1- 3600).

Configuring the Auth Profiles Tab

▶ *Network > Virtual Router > RIP > Auth Profiles*

The following table describes the settings for the **Auth Profiles** tab.

Table 85. RIP Settings – Auth Profiles Tab

Field	Description
Auth Profiles	
Profile Name	Enter a name for the authentication profile to authenticate RIP messages. To authenticate RIP messages, first define the authentication profiles and then apply them to interfaces on the **RIP** tab.
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.

Configuring the Export Rules Tab

▶ *Network > Virtual Router > RIP > Export Rules*

The following table describes the settings for the **Export Rules** tab.

Table 86. RIP Settings – Export Rules Tab

Field	Description
Export Rules	
Export Rules	(Read-only) Displays the rules that apply to routes sent by the virtual router to a receiving router. • **Allow Redistribute Default Route**—Select the check box to permit the firewall to redistribute its default route to peers. • **Redistribution Profile**—Select a redistribution profile that allows you to modify route redistribution, filter, priority, and action based on the desired network behavior. Refer to "Configuring the Redistribution Profiles Tab".

Configuring the OSPF Tab

▶ *Network > Virtual Router > OSPF*

Configuring the Open Shortest Path First (OSPF) protocol requires configuring the following general settings:

Table 87. Virtual Router Settings - OSPF Tab

Field	Description
Enable	Select the check box to enable the OSPF protocol.
Reject Default Route	Select the check box if you do not want to learn any default routes through OSPF. Selecting the check box is recommended, especially for static routes.
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.

In addition, settings on the following tabs must be configured:

- **Areas** tab: See "Configuring the Areas Tab".
- **Auth Profiles** tab: See "Configuring the Auth Profiles Tab".
- **Export Rules** tab: See".Configuring the Export Rules Tab".
- **Advanced** tab: See "Configuring the Advanced Tab".

Configuring the Areas Tab

▶ *Network > Virtual Router > OSPF > Areas*

The following table describes the settings for the **Areas** tab.

Table 88. OSPF Settings – Areas Tab

Field	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 (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.

Table 88. OSPF Settings – Areas Tab (Continued)

Field	Description
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. • **Passive**—Select the check box 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 (0-65535). • **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. • **Hello Interval (sec)**—Interval at which the OSPF process sends hello packets to its directly connected neighbors. Range: 0-3600 seconds. Default: 10 seconds. • **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: 3-20. Default: 4. • **Retransmit Interval (sec)**—Length of time that OSPF waits to receive a link-state advertisement (LSA) from a neighbor before OSPF retransmits the LSA. Range: 0-3600 seconds. Default: 10 seconds. • **Transit Delay (sec)**—Length of time that an LSA is delayed before it is sent out of an interface. Range: 0-3600 seconds. Default: 1 second. • **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: 1-10 seconds. Default: 10 seconds.

Table 88. OSPF Settings – Areas Tab (Continued)

Field	Description
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.

Configuring the Auth Profiles Tab

▶ *Network > Virtual Router > OSPF > Auth Profiles*

The following table describes the settings for the **Auth Profiles** tab.

Table 89. OSPF Settings – Auth Profiles Tab

Field	Description
Auth Profiles	
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.

.Configuring the Export Rules Tab

▶ *Network > Virtual Router > OSPF > Export Rules*

The following table describes the settings for the **Export Rules** tab.

Table 90. OSPF Settings – Auth Profiles Tab

Field	Description
Export Rules	
Allow Redistribute Default Route	Select the check box to permit redistribution of default routes through OSPF.

Table 90. OSPF Settings – Auth Profiles Tab (Continued)

Field	Description
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	Specify the route metric to be associated with the exported route and used for path selection (optional, range 1-65535).

Configuring the Advanced Tab

▶ *Network > Virtual Router > OSPF > Advanced*

The following table describes the settings for the **Advanced** tab.

Table 91. OSPF Settings – Advanced Tab

Field	Description
Advanced	
RFC 1583 Compatibility	Select the check box to ensure compatibility with RFC 1583.
Timers	• **SPF Calculation Delay (sec)**—This option 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 should continue to forward to this firewall adjacencies are being re-established or the router is being restarted. Range: 5 - 1800 seconds. Default: 120 seconds. • **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: 5 - 1800 seconds. Default: 140 seconds.

Configuring the OSPFv3 Tab

▶ *Network > Virtual Router > OSPFv3*

Configuring the Open Shortest Path First v3 (OSPFv3) protocol requires configuring the following general settings:

Table 92. Virtual Router Settings - OSPF Tab

Field	Description
Enable	Select the check box to enable the OSPF protocol.
Reject Default Route	Select the check box if you do not want to learn any default routes through OSPF. Selecting the check box is recommended, especially for static routes.
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.

In addition, settings on the following tabs must be configured:

- **Areas** tab: See “Configuring the Areas Tab”.
- **Auth Profiles** tab: See “Configuring the Auth Profiles tab”.
- **Export Rules** tab: See “Configuring the Export Rules Tab”.
- **Advanced** tab: See “Configuring the Advanced Tab”.

Configuring the Areas Tab

▶ *Network > Virtual Router > OSPFv3 > Areas*

The following table describes the settings for the **Areas** tab.

Table 93. Virtual Router Settings - Areas Tab

Field	Description
Authentication	Select the name of the Authentication profile that you want to specify for this OSPF 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 (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.

Table 93. Virtual Router Settings - Areas Tab (Continued)

Field	Description
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 the check box 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 (0-65535). • **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. • **Hello Interval (sec)**—Interval at which the OSPF process sends hello packets to its directly connected neighbors. Range: 0-3600 seconds. Default: 10 seconds. • **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: 3-20. Default: 4. • **Retransmit Interval (sec)**—Length of time that OSPF waits to receive a link-state advertisement (LSA) from a neighbor before OSPF retransmits the LSA. Range: 0-3600 seconds. Default: 10 seconds. • **Transit Delay (sec)**—Length of time that an LSA is delayed before it is sent out of an interface. Range: 0-3600 seconds. Default: 1 second. • **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: 1-10 seconds. Default: 10 seconds. • **Neighbors**—For p2pmp interfaces, enter the neighbor IP address for all neighbors that are reachable through this interface.

Table 93. Virtual Router Settings - Areas Tab (Continued)

Field	Description
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 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.

Configuring the Auth Profiles tab

▶ *Network > Virtual Router > OSPFv3 > Auth Profiles*

The following table describes the settings for the **Auth Profiles** tab.

Table 94. OSPFv3 Settings – Auth Profiles Tab

Field	Description
Auth Profiles	
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**—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.

Table 94. OSPFv3 Settings – Auth Profiles Tab (Continued)

Field	Description
Encryption	Specify one of the following: • **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. Not available if the AH protocol was chosen.
Key/Confirm Key	Enter and confirm an encryption key.

Configuring the Export Rules Tab

▶ *Network > Virtual Router > OSPF > Export Rules*

The following table describes the settings for the **Export Rules** tab.

Table 95. OSPF Settings – Auth Profiles Tab

Field	Description
Export Rules	
Allow Redistribute Default Route	Select the check box 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	Specify the route metric to be associated with the exported route and used for path selection (optional, range 1-65535).

Configuring the Advanced Tab

▶ *Network > Virtual Router > OSPF > Advanced*

The following table describes the settings for the **Advanced** tab.

Table 96. OSPF Settings – Advanced Tab

Field	Description
Advanced	
Disable Transit Routing for SPF Calculation	Select this check box if you want to set the R-bit in router LSAs sent from this device to indicate that the router is not active. When in this state, the device participates in OSPFv3 but other routers do not send transit traffic. In this state, local traffic will still be forwarded to the device. This is useful while performing maintenance with a dual-homed network because traffic can be re-routed around the device while it can still be reached.

Table 96. OSPF Settings – Advanced Tab (Continued)

Field	Description
Timers	• **SPF Calculation Delay (sec)**—This option 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 should continue to forward to this firewall adjacencies are being re-established or the router is being restarted. Range: 5 - 1800 seconds. Default: 120 seconds. • **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: 5 - 1800 seconds. Default: 140 seconds.

Configuring the BGP Tab

▶ *Network > Virtual Router > BGP*

Configuring the Border Gateway Protocol (BGP) protocol requires configuring the following settings:

Table 97. Virtual Router Settings - BGP Tab

Field	Description
Enable	Select the check box 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 1-4294967295).

In addition, settings on the following tabs must be configured:

- **General** tab: See “Configuring the General Tab”.
- **Advanced** tab: See “Configuring the Advanced Tab”.

- **Peer Group** tab: See "Configuring the Peer Group Tab".
- **Import** tab: See "Configuring the Import and Export Tabs".
- **Export** tab: See "Configuring the Import and Export Tabs".
- **Conditional Adv** tab: See "Configuring the Conditional Adv Tab".
- **Aggregate** tab: See "Configuring the Conditional Adv Tab".
- **Redist Rules** tab: See "Configuring the Redist Rules Tab".

Configuring the General Tab

▶ *Network > Virtual Router > BGP > General*

The following table describes the settings for the **General** tab.

Table 98. BGP Settings – General Tab

Field	Description
General Tab	
Reject Default Route	Select the check box to ignore any default routes that are advertised by BGP peers.
Install Route	Select the check box 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 than can be used 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	Click **Add** to include a new authentication 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. Click the icon to delete a profile.

Configuring the Advanced Tab

▶ *Network > Virtual Router > BGP > Advanced*

The following table describes the settings for the **Advanced** tab:

Table 99. BGP Settings – Advanced Tab

Field	Description
Advanced Tab	
Graceful Restart	Activate the graceful restart option. • **Stale Route Time**—Specify the length of time that a route can stay in the stale state (range 1-3600 seconds, default 120 seconds). • **Local Restart Time**—Specify the length of time that the local device takes to restart. This value is advertised to peers (range 1-3600 seconds, default 120 seconds). • **Max Peer Restart Time**—Specify the maximum length of time that the local device accepts as a grace period restart time for peer devices (range 1-3600 seconds, default 120 seconds).
Reflector Cluster ID	Specify an IPv4 identifier to represent the reflector cluster.
Confederation Member AS	Specify the identifier for the AS confederation to be presented as a single AS to external BGP peers.
Dampening Profiles	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 0.0-1000.0, default 1.25). • **Reuse**—Specify a route withdrawal threshold below which a suppressed route is used again (range 0.0-1000.0, default 5). • **Max. Hold Time**—Specify the maximum length of time that a route can be suppressed, regardless of how unstable it has been (range 0-3600 seconds, default 900 seconds). • **Decay Half Life Reachable**—Specify the length of time after which a route's stability metric is halved if the route is considered reachable (range 0-3600 seconds, default 300 seconds). • **Decay Half Life Unreachable**—Specify the length of time after which a route's stability metric is halved if the route is considered unreachable (range 0-3600 seconds, default 300 seconds). Click the icon to delete a profile.

Configuring the Peer Group Tab

▶ *Network > Virtual Router > BGP > Peer Group*

The following table describes the settings for the **Peer Group** tab:

Table 100. BGP Settings – Peer Group Tab

Field	Description
Peer Group Tab	
Name	Enter a name to identify the peer.
Enable	Select to activate the peer.
Aggregated Confed AS Path	Select the check box to include a path to the configured aggregated confederation AS.

Table 100. BGP Settings – Peer Group Tab (Continued)

Field	Description
Soft Reset with Stored Info	Select the check box 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).
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 local forwarding table. • **use-self**—Replace the Next Hop address with this router's IP address to ensure that it will be in the forwarding path.

Table 100. BGP Settings – Peer Group Tab (Continued)

Field	Description
Peer	To add a new peer, click **New** and configure the following settings: • **Name**—Enter a name to identify the peer. • **Enable**—Select to activate the peer. • **Peer AS**—Specify the AS of the peer. • **Local Address**—Choose a firewall interface and local IP address. • **Connection Options**—Specify the following options: – **Auth Profile**—Select the profile. – **Keep Alive Interval**—Specify an interval after which routes from a peer are suppressed according to the hold time setting (range 0-1200 seconds, default 30 seconds). – **Multi Hop**—Set the time-to-live (TTL) value in the IP header (range 1-255, default 0). The default value of 0 means 2 for eBGP and 255 for iBGP. – **Open Delay Time**—Specify the delay time between opening the peer TCP connection and sending the first BGP open message (range 0-240 seconds, default 0 seconds). – **Hold Time**—Specify the period of time that may elapse between successive KEEPALIVE or UPDATE messages from a peer before the peer connection is closed. (range 3-3600 seconds, default 90 seconds). – **Idle Hold Time**—Specify the time to wait in the idle state before retrying connection to the peer (range 1-3600 seconds, default 15 seconds). • **Peer Address**—Specify the IP address and port of the peer. • **Advanced Options**—Configure the following settings: – **Reflector Client**—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 - 100000 or unlimited). • **Incoming Connections/Outgoing Connections**—Specify the incoming and outgoing port numbers and select the Allow check box to allow traffic to or from these ports.

Configuring the Import and Export Tabs

▶ *Network > Virtual Router > BGP > Import*

▶ *Network > Virtual Router > BGP > Export*

The following table describes the settings for the **Import** and **Export** tabs:

Table 101. BGP Settings – Import and Export Tabs

Field	Description
Import Rules/Export Rules Tabs	
Import Rules/Export Rules	Click the BGP **Import Rules** or **Export Rules** subtab. To add a new rule, click **Add** and configure the following settings. • **General** subtab: – **Name**—Specify a name to identify the rule. – **Enable**—Select to activate the rule. – Used **by**—Select the peer groups that will use this rule. • **Match** subtab: – **AS-Path Regular Expression**—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. – **Address Prefix**—Specify IP addresses or prefixes for route filtering. – **MED**—Specify a MED value for route filtering. – **Next Hop**—Specify next hop routers or subnets for route filtering. – **From Peer**—Specify peer routers for route filtering. • **Action** subtab: – **Action**—Specify an action (**Allow** or **Deny**) to take when the match conditions are met. – **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- 65535). – **Weight**—Specify a weight value, only if the action is **Allow** (0- 65535). – **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**. – **Dampening**—Specify the dampening parameter, only if the action is **Allow**. Click the icon to delete a group. Click **Clone** to add a new group with the same settings as the selected group. A suffix is added to the new group name to distinguish it from the original group.

Configuring the Conditional Adv Tab

▶ *Network > Virtual Router > BGP > Conditional Adv*

The following table describes the settings for the **Conditional Adv** tab:

Table 102. BGP Settings – Conditional Adv Tabs

Field	Description
Conditional Adv Tab	The BGP conditional advertisement feature allows you to control what route to advertise in the event that a different route is not available in the local BGP routing table (LocRIB), indicating a peering or reachability failure. This is useful in cases where you want to try and force routes to one AS over another, for example if you have links to the Internet through multiple ISPs and you want traffic to be routed to one provider instead of the other unless there is a loss of connectivity to the preferred provider. With conditional advertising, you can configure a non-exist filter that matches the prefix of the preferred route. If any route matching the non-exist filter is not found in the local BGP routing table, only then will the device 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 and then click **Add**. The following describes how to configure the values in the fields.
Policy	Specify the policy name for this conditional advertisement rule.
Enable	Select the check box to enable BGP conditional advertisement.
Used By	Click **Add** and select the peer groups that will use this conditional advertisement policy.
Non Exist Filters Subtab	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. Click **Add** to create a non-exist filter. • **Non Exist Filters**—Specify a name to identify this filter. • **Enable**—Select to activate the filter. • **AS-Path Regular Expression**—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 MED value for route filtering. • **Address Prefix**—Click **Add** and then specify the exact NLRI prefix for the preferred route. • **Next Hop**—Specify next hop routers or subnets for route filtering. • **From Peer**—Specify peer routers for route filtering.

Table 102. BGP Settings – Conditional Adv Tabs (Continued)

Field	Description
Advertise Filters Subtab	Use this tab to specify the prefix(es) of the route in the Local-RIB routing table that should be advertised in the event that the route in the non-exist filter is not available in the local routing table. If a prefix is going to be advertised and does not match a Non Exist filter, the advertisement will occur. Click **Add** to create an advertise filter. • **Advertise Filters**—Specify a name to identify this filter. • **Enable**—Select to activate the filter. • **AS-Path Regular Expression**—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 MED value for route filtering. • **Address Prefix**—Click **Add** and then specify the exact 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.

Configuring the Aggregate Tab

▶ *Network > Virtual Router > BGP > Aggregate*

The following table describes the settings for the **Aggregate** tab:

Table 103. BGP Settings – Aggregate Tabs

Field	Description
Aggregate Tabs	
Name	Enter a name for the aggregation configuration.
Suppress Filters	Define the attributes that will cause the matched routes to be suppressed.
Advertise Filters	Define the attributes for the advertise filters that will ensure that any router that matches the defined filter will be advertised to peers.
Aggregate Route Attributes	Define the attributes that will be used to match routes that will be aggregated.

Configuring the Redist Rules Tab

▶ *Network > Virtual Router > BGP > Redist Rules*

The following table describes the settings for the **Redist Rules** tab:

Table 104. BGP Settings – Redist Rules

Field	Description
Redist Rules Tab	
Name	Select the name of a redistribution profile.
Allow Redistribute Default Route	Select the check box to permit the firewall to redistribute its default route to BGP peers.
Redist Rules	To add a new rule, click **Add**, configure the settings, and click **Done**. The parameters are described above in this table for the **Import Rules** and **Export Rules** tabs. Click the icon to delete a rule.

Configuring the Multicast Tab

▶ *Network > Virtual Router > Multicast*

Configuring Multicast protocols requires configuring the following standard settings:

Table 105. Virtual Router Settings - Multicast Tab

Field	Description
Enable	Select the check box to enable multicast routing.

In addition, settings on the following tabs must be configured:

- **Rendezvous Point** tab: See "Configuring the Rendezvous Point Tab".
- **Interfaces** tab: See "Configuring the Interfaces Tab".
- **SPT Threshold** tab: See "Configuring the SPT Threshold Tab".
- **Source Specific Address Space** tab: See "Configuring the Source Specific Address Tab".

Configuring the Rendezvous Point Tab

▶ *Network > Virtual Router > Multicast > Rendezvous Point*

The following table describes the settings for the **Rendezvous Point** tab:

Table 106. Multicast Settings – Rendezvous Point Tab

Field	Description
Rendezvous Point Subtab	
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 lists. Select the **Override learned RP for the same group** check box 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 the check box 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.

Configuring the Interfaces Tab

▶ *Network > Virtual Router > Multicast > Interfaces*

The following table describes the settings for the **Interfaces** tab:

Table 107. Multicast Settings – Interfaces Tab

Field	Description
Interfaces Subtab	
Name	Enter a name to identify an interface group.
Description	Enter an optional description.
Interface	Click **Add** to specify one or more firewall interfaces.
Group Permissions	Specify general rules for multicast traffic: • **Any Source**—Click **Add** to specify a list of multicast groups for which PIM-SM traffic is permitted. • **Source-Specific**—Click **Add** to specify a list of multicast group and multicast source pairs for which PIM-SSM traffic is permitted.

Table 107. Multicast Settings – Interfaces Tab (Continued)

Field	Description
IGMP	Specify rules for IGMP traffic. IGMP must be enabled for host facing interfaces (IGMP router) or for IGMP proxy host interfaces. • **Enable**—Select the check box to enable the IGMP configuration. • **IGMP Version**—Choose version 1, 2, or 3 to run on the interface. • **Enforce Router-Alert IP Option**—Select the check box to require the router-alert IP option when speaking IGMPv2 or IGMPv3. This option must be disabled for compatibility with IGMPv1. • **Robustness**—Choose an integer value to account for packet loss on a network (range 1-7, default 2). If packet loss is common, choose a higher value. • **Max Sources**—Specify the maximum number of source-specific memberships allowed on this interface (0 = unlimited). • **Max Groups**—Specify the maximum number of groups allowed on this interface. • **Query Configuration**—Specify the following: – **Query interval**—Specify the interval at which general queries are sent to all hosts. – **Max Query Response Time**—Specify the maximum time between a general query and a response from a host. – **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 the check box to leave the group immediately when a leave message is received.
PIM configuration	Specify the following Protocol Independent Multicast (PIM) settings: • **Enable**—Select the check box to allow this interface to receive and/or forward PIM messages • **Assert Interval**—Specify the interval between PIM assert messages. • **Hello Interval**—Specify the interval between PIM hello messages. • **Join Prune Interval**—Specify the interval between PIM join and prune messages (seconds). Default is 60. • **DR Priority**—Specify the designated router priority for this interface • **BSR Border**—Select the check box to use the interface as the bootstrap border. • **PIM Neighbors**—Click **Add** to specify the list of neighbors that will communicate with using PIM.

Configuring the SPT Threshold Tab

▶ *Network > Virtual Router > Multicast > SPT Threshold*

The following table describes the settings for the **SPT Threshold** tab:

Table 108. Multicast Settings – SPT Threshold Tab

Field	Description
SPT Threshold Subtab	
Name	The Shortest Path Tree (SPT) threshold defines the throughput rate (in kbps) at which multicast routing will switch from shared tree distribution (sourced from the rendezvous point) to source tree distribution. Click **Add** to specify the following SPT settings: • **Multicast Group Prefix**—Specify the multicast IP address/prefix for which the SPT will be switched to source tree distribution when the throughput reaches the desired threshold (kbps). • **Threshold**—Specify the throughput at which we'll switch from shared tree distribution to source tree distribution

Configuring the Source Specific Address Tab

▶ *Network > Virtual Router > Multicast > Source Specific Address Space*

The following table describes the settings for the **Source Specific Address Space** tab:

Table 109. Multicast Settings – Source Specific Address Space Tab

Field	Description
Source Specific Address Space Subtab	
Name	Defines the multicast groups for which the firewall will provide source-specific multicast (SSM) services. Click **Add** to specify the following settings for source-specific addresses: • **Name**—Enter a name to identify this group of settings. • **Group**—Specify groups for the SSM address space. • **Included**—Select this check box to include the specified groups in the SSM address space.

Defining Security Zones

▶ *Network > Zones*

In order for a firewall interface to be able to process traffic, it must be assigned to a security zone. To define security zones, click **New** and specify the following information:

Table 110. Security Zone Settings

Field	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. Use only letters, numbers, spaces, hyphens, periods, and underscores.

Table 110. Security Zone Settings (Continued)

Field	Description
Location	This field only appears if the device supports multiple virtual systems (vsys) and that capability is enabled. Select the vsys that applies to this zone.
Type	Select a zone type (Layer2, Layer3, Virtual Wire, Tap, or External virtual system) to list 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. The External virtual system type is for communications among virtual systems in the firewall. Each interface can belong to one zone in one virtual system.
Zone Protection Profiles	Select a profile that specifies how the security gateway responds to attacks from this zone. To add new profiles, refer to “Defining Zone Protection Profiles”.
Log Setting	Select a log forwarding profile for forwarding zone protection logs to an external system. If you have a log forwarding profile that is named *default*, that profile will be automatically selected for this field 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 field is populated automatically), click **New** (refer to “Log Forwarding”).
Enable User Identification	If you configured User-ID™ to perform IP address to username mapping (discovery), select this check box to apply the mapping information to traffic in this zone. If you clear the check box, firewall logs, reports, and policies will exclude user mapping information for traffic within the zone. By default, if you select this check box, 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**. Note that 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 the **Enable User Identification** check box. To define the monitored range, see the PAN-OS 7.0 Administrator's Guide.
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: 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. Note that you can only include subnetworks that fall within the network range that User-ID monitors. To define the monitored range, see the PAN-OS 7.0 Administrator's Guide.

Table 110. Security Zone Settings (Continued)

Field	Description
User Identification ACL Exclude List	To exclude user mapping information for a subset of the subnetworks in the **Include List**, for each subnetwork to exclude, click **Add** and select an address (or address group) object or type the IP address range. 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.

Building Blocks of 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 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 having to wait for the routing protocol or RIB table to elect an alternative path. This can help reduce down time when links fail.

ECMP load balancing is done at the session level, not at the packet level. This means that the firewall chooses an equal-cost path at the start of a new session, not each time a packet is received.

Note: *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 following:

Table 111 ECMP

Field	Description
Enable	Click **Enable** to enable ECMP. Enabling, disabling, or changing ECMP requires that you restart the firewall, which might cause sessions to be terminated.
Symmetric Return	Optionally click the **Symmetric Return** check box 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.

Table 111 ECMP

Field	Description
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: 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. • **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**—Optionally click **Use Source/Destination Ports** to include the ports in the hash calculation, in addition to the source and destination IP addresses. 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.

More Runtime Stats for a Virtual Router

Clicking on the More Runtime Stats link on a row for a Virtual Router opens a window that displays information about that Virtual Router. The window displays the following tabs:

- **Routing** tab: See “Routing Tab”.
- **RIP** tab: See “RIP Tab”.
- **BGP** tab: See “BGP Tab”.
- **Multicast** tab: See “Multicast Tab”.

Routing Tab

The following table describes the virtual router’s Runtime Stats for Routing.

Table 112 Routing Runtime Stats

Field	Description
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.
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.

RIP Tab

The following table describes the virtual router's Runtime Stats for RIP.

Table 113 RIP Runtime Stats

Field	Description
Summary Subtab	
Interval Seconds	Number of seconds in an interval; this value affects the 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 route is deleted from the routing table.
Interface Subtab	
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.

Table 113 RIP Runtime Stats (Continued)

Field	Description
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 Subtab	
Peer Address	IP address of a peer to the virtual router's RIP interface.
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.

Table 114 BGP Runtime Stats

Field	Description
Summary Subtab	
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.

Table 114 BGP Runtime Stats (Continued)

Field	Description
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.
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 Subtab	
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 Subtab	
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.
Local RIB Subtab	
Prefix	Network prefix and subnet mask in the Local Routing Information Base.
Flag	* indicates the route was chosen as the best BGP route.

Table 114 BGP Runtime Stats (Continued)

Field	Description
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 Subtab	
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 advertising the route suggests to an external AS. A lower MED is preferred over a higher MED.
Adv. Status	Advertised status of the route.
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.

Table 115 Multicast Runtime Stats

Field	Description
FIB Subtab	
Group	Multicast group address that the VR will forward.
Source	Multicast source address.
Incoming Interfaces	Indicates interfaces where the multicast traffic comes in on the VR.

Table 115 Multicast Runtime Stats (Continued)

Field	Description
IGMP Interface Subtab	
Interface	Interface that has IGMP enabled.
Version	Version 1, 2, or 3 of Internet Group Management Protocol (IGMP).
Querier	IP address of the IGMP querier on that interface.
Querier Up Time	Length of time that IGMP querier has been up.
Querier Expiry Time	Time remaining before the current the Other Querier Present timer expires.
Robustness	Robustness variable of the IGMP interface.
Groups Limit	Number of multicast groups allowed on the interface.
Sources Limit	Number of multicast sources allowed on the interface.
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 Subtab	
Interface	Name of an interface to which the membership belongs.
Group	IP Multicast group address.
Source	Source address of multicast traffic.
Up Time	Length of time this membership been up.
Expiry Time	Length of time remaining before membership expires.
Filter Mode	Include or exclude the source. VR is configured to include all traffic, or only traffic from this source (include), or traffic from any source except this one (exclude).
Exclude Expiry	Time 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 Subtab	
Group	IP address of the group mapped to a Rendezvous Point.
RP	IP address of Rendezvous Point for the group.
Origin	Indicates where the VR learned of the RP.
PIM Mode	ASM or SSM.
Inactive	Indicates that the mapping of the group to the RP is inactive.
PIM Interface Subtab	

Table 115 Multicast Runtime Stats (Continued)

Field	Description
Interface	Name of interface participating in PIM.
Address	IP address of the interface.
DR	IP address of the Designated Router on the interface.
Hello Interval	Hello interval configured (in seconds).
Join/Prune Interval	Join/Prune interval configured (in seconds).
Assert Interval	Assert interval configured (in seconds).
DR Priority	Priority configured for the Designated Router.
BSR Border	Yes or no.
PIM Neighbor Subtab	
Interface	Name of interface in the VR.
Address	IP address of the neighbor.
Secondary Address	Secondary IP address of the neighbor.
Up Time	Length of time the neighbor has been up.
Expiry Time	Length of time remaining before the neighbor expires because the VR is not receiving hello packets from the neighbor.
Generation ID	Value that the VR received from the neighbor in the last PIM hello message received on this interface.
DR Priority	Designated Router priority that the VR received in the last PIM hello message from this neighbor.

Configuring VLAN Support

▶ *Network > VLANs*

The firewall supports VLANs that conform to the IEEE 802.1Q standard. Each Layer 2 interface that is defined on the firewall must 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.

Table 116. VLAN Settings

Field	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 VLAN interface to allow traffic to be routed outside the VLAN. To define a VLAN interface, see "Configure a VLAN Interface".
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.

Configuring 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"*
How do I configure a DHCP Server?	▶ *"Building Blocks of DHCP Server"*
How do I configure a DHCP Relay Agent?	▶ *"Building Blocks of DHCP Relay"*
How can I configure a DHCP Client?	▶ *"Building Blocks of DHCP Client"*
Show me a basic example.	▶ *"Example: Configure a DHCP Server with Custom Options"*
Looking for more?	**See** DHCP**.**

DHCP Overview

▶ *Network > DHCP*

DHCP uses a client-server model of communication. This model consists of three roles that the device can fulfill: DHCP client, DHCP server, and DHCP relay agent.

- A device acting as a DHCP client (host) can request an IP address and other configuration settings from a DHCP server. Users on client devices 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 device 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 device 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 device. 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 device is used for something crucial and must keep the same IP address, even if the device 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 device. You might reserve a few addresses from the pool and statically assign them to a fax and printer, for example, without using DHCP.

Link to related topics:

- "Building Blocks of DHCP Server"
- "Building Blocks of DHCP Relay"
- "Building Blocks of DHCP Client"
- "Example: Configure a DHCP Server with Custom Options"

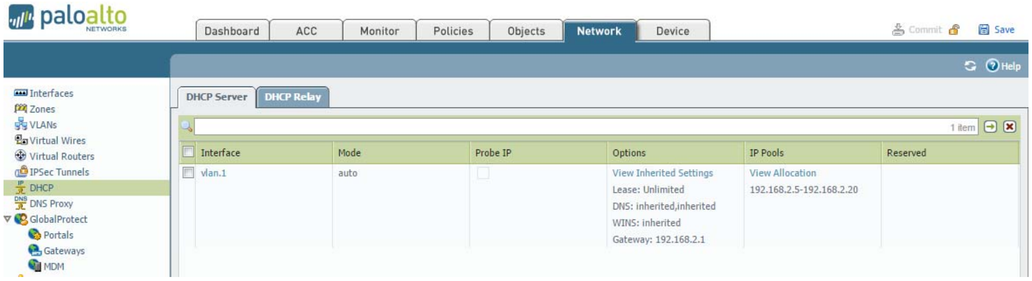
Building Blocks of DHCP Server

▶ *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. The resulting DHCP server settings will look similar to this:

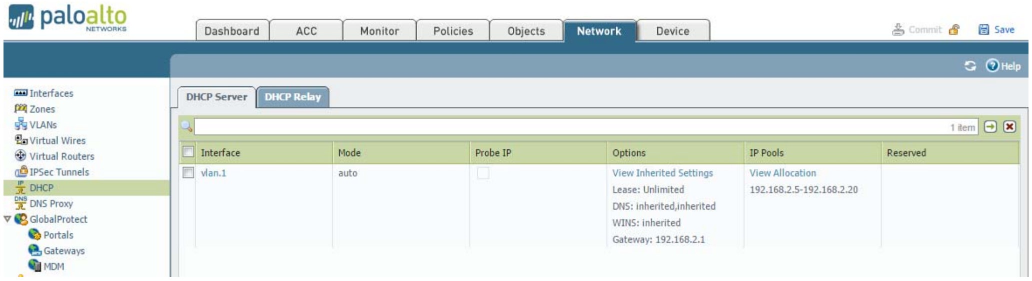
Table 117. DHCP Server Settings



Interface	Mode	Probe IP	Options	IP Pools	Reserved
vlan.1	auto	□	View Inherited Settings Lease: Unlimited DNS: inherited,inherited WINS: inherited Gateway: 192.168.2.1	View Allocation 192.168.2.5-192.168.2.20	

Field	Configured In	Description
Interface	DHCP Server	Name of the interface that will serve as the DHCP server.
Mode	DHCP Server	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	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 device 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, the Probe IP column in the display will have a check mark.
Lease	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	Lease	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	Lease	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 device associated with that MAC address when that device requests an IP address through DHCP.

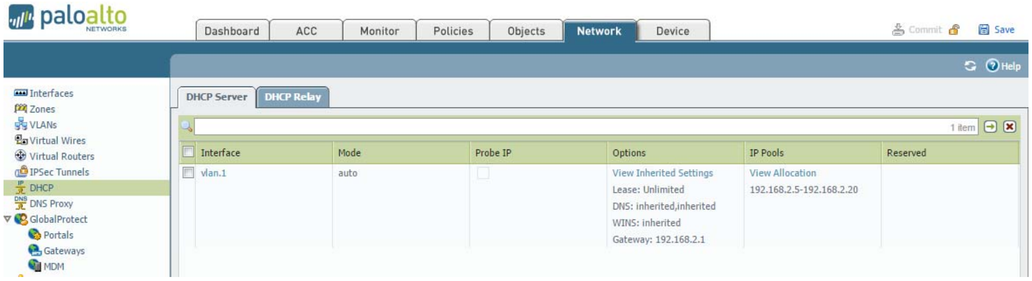
Table 117. DHCP Server Settings



□	Interface	Mode	Probe IP	Options	IP Pools	Reserved
□	vlan.1	auto	□	View Inherited Settings Lease: Unlimited DNS: inherited,inherited WINS: inherited Gateway: 192.168.2.1	View Allocation 192.168.2.5-192.168.2.20	

Field	Configured In	Description
Inheritance Source	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 device 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	Options	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.
Gateway	Options	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	Options	Specify the network mask that applies to the addresses in the **IP Pools**.

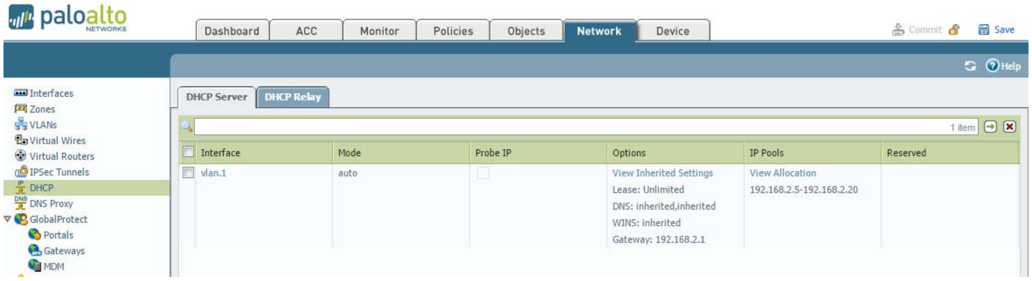
Table 117. DHCP Server Settings



Interface	Mode	Probe IP	Options	IP Pools	Reserved
☐ vlan.1	auto	☐	View Inherited Settings Lease: Unlimited DNS: inherited,inherited WINS: inherited Gateway: 192.168.2.1	View Allocation 192.168.2.5-192.168.2.20	

Field	Configured In	Description
Options	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.

Table 117. DHCP Server Settings



Interface	Mode	Probe IP	Options	IP Pools	Reserved
vlan.1	auto	□	View Inherited Settings Lease: Unlimited DNS: inherited,inherited WINS: inherited Gateway: 192.168.2.1	View Allocation 192.168.2.5-192.168.2.20	

Field	Configured In	Description
Custom DHCP options	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 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. Click **Inherited from DCHP server inheritance source** to have the server inherit the value for that option code from the inheritance source instead of you entering an **Option Value**. As an alternative to the check box, 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.

Building Blocks of DHCP Relay

▶ *Network > DHCP > DHCP Relay*

Before configuring a firewall interface as a DHCP relay agent, 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. The interface can forward messages to a maximum of four external DHCP servers. A client DHCPDISCOVER message is sent to all configured servers, and the DHCPOFFER message of the first server that responds is relayed back to the requesting client.

Table 118. DHCP Relay Settings

Field	Configured In	Description
Interface	DHCP Relay	Name of the interface that will be the DHCP relay agent.
IPv4 / IPv6	DHCP Relay	Select the type of DHCP server and IP address you will specify.

Table 118. DHCP Relay Settings

Field	Configured In	Description
DHCP Server IP Address	DHCP Relay	Enter the IP address of the DHCP server to and from which you will relay DHCP messages.
Interface	DHCP Relay	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.

Building Blocks of 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.

Table 119. DHCP Client Settings

Field	Configured In	Description
Type	IPv4	Click the radio button for **DHCP Client** and check **Enable** to configure the interface as a DHCP client.
Automatically create default route pointing to default gateway provided by server	IPv4	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	IPv4	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. There is no default metric.
Show DHCP Client Runtime Info	IPv4	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).

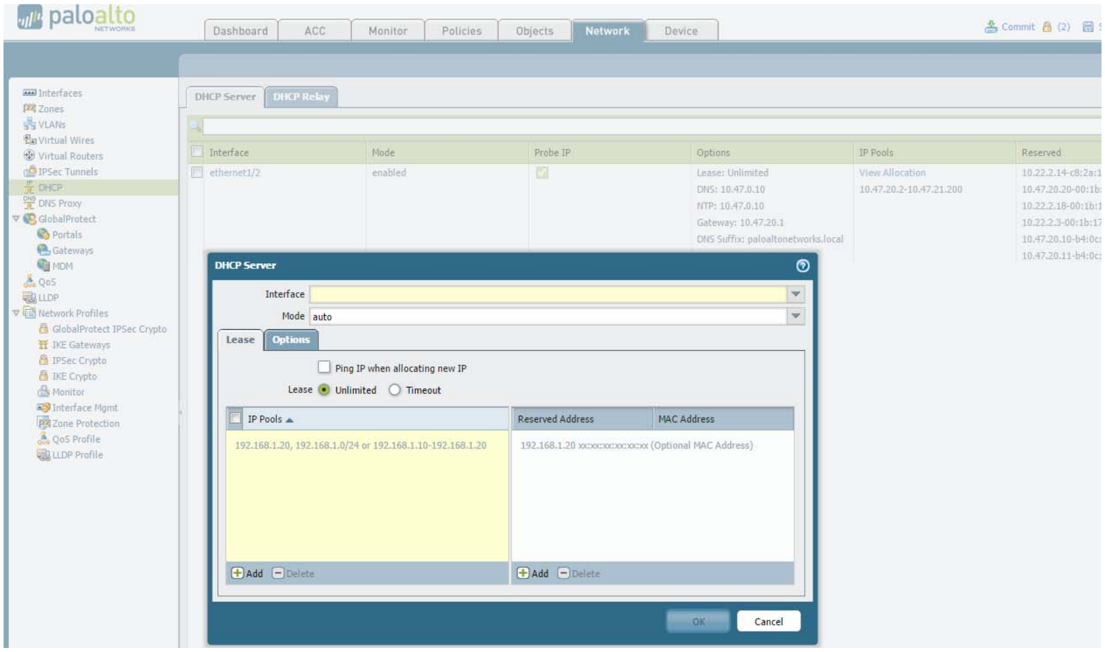
Example: Configure a DHCP Server with Custom Options

In the following example, an interface on the firewall is configured as a DHCP server. The DHCP server is configured with Options 66 and 150 to provide information about TFTP servers that provide configurations for Cisco IP phones. This means that when clients request

Option 66 and 150 from the server, the server will send these option values in its response. Cisco IP phones receive their configuration from a TFTP server. DHCP option 66 provides the host name for a TFTP server; option 150 provides the IP address of a TFTP server.

Configure a DHCP Server with Custom Options

1. Select **Network > DHCP > DHCP Server**.
2. Select the interface that is to serve as the DHCP Server.
3. On the **Lease** tab, specify the **Timeout** as 1 day.
4. Specify the range of IP addresses in the **IP Pools** that the server can assign to clients.



Interface	Mode	Probe IP	Options	IP Pools	Reserved
ethernet1/2	enabled	☑	Lease: Unlimited DNS: 10.47.0.10 NTP: 10.47.0.10 Gateway: 10.47.20.1 DNS Suffix: paloaltonetworks.local	View Allocation 10.47.20.2-10.47.21.200	10.22.2.14-c8:2a:1 10.47.20.20-00:1b: 10.22.2.18-00:1b:1 10.22.2.3-00:1b:17 10.47.20.10-b4:0c: 10.47.20.11-b4:0c:

DHCP Server

Interface

Mode auto

Lease | Options

□ Ping IP when allocating new IP

Lease ● Unlimited ○ Timeout

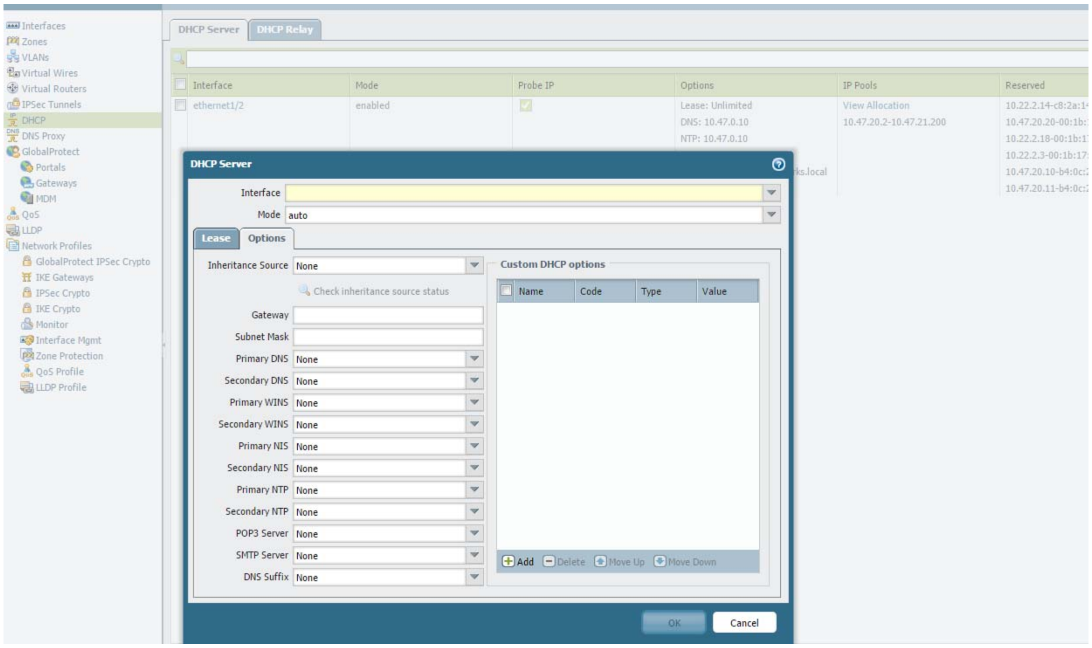
IP Pools ▲
192.168.1.20, 192.168.1.0/24 or 192.168.1.10-192.168.1.20

Reserved Address	MAC Address
192.168.1.20 xx:xx:xx:xx:xx:xx (Optional MAC Address)	

Configure a DHCP Server with Custom Options

5. On the **Options** tab, enter the gateway address and subnet mask for the network.

6. Enter the addresses of the servers that this DHCP server will send to clients.



Interface	Mode	Probe IP	Options	IP Pools	Reserved
ethernet1/2	enabled	☑	Lease: Unlimited DNS: 10.47.0.10 NTP: 10.47.0.10 ks.local	View Allocation 10.47.20.2-10.47.21.200	10.22.2.14-c8:2a:1 10.47.20.20-00:1b: 10.22.2.18-00:1b:1 10.22.2.3-00:1b:17 10.47.20.10-b4:0c: 10.47.20.11-b4:0c:

Interface
Mode: auto

Inheritance Source: None
Gateway
Subnet Mask
Primary DNS: None
Secondary DNS: None
Primary WINS: None
Secondary WINS: None
Primary NIS: None
Secondary NIS: None
Primary NTP: None
Secondary NTP: None
POP3 Server: None
SMTP Server: None
DNS Suffix: None

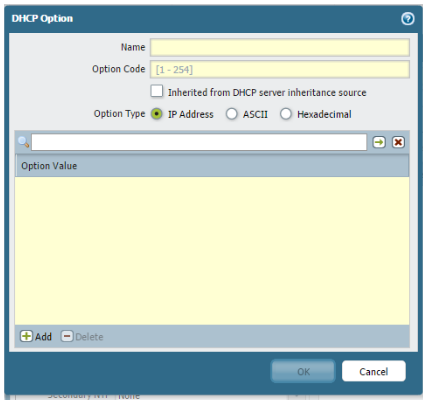
☐	Name	Code	Type	Value

Configure a DHCP Server with Custom Options

7. To enter a custom DHCP option, click **Add**. For this example, enter a name for the option, such as `VoIP Phones Hostname` and the option code `66`. The name of the option is not sent to the client; it is for ease of identification on the server.

8. Select **ASCII**.

9. Click **Add** to enter the option value `TFTPserver10` and click **OK**.



DHCP Option

Name

Option Code [1 - 254]

□ Inherited from DHCP server inheritance source

Option Type ● IP Address ○ ASCII ○ Hexadecimal

10. To enter another DHCP Option, click **Add**. Enter a different name, such as `VoIP Phones IP Address` and the option code `150`. The name must be different from the first name because the types of data are different.

11. Select **IP Address**.

12. Click **Add** to enter the option value `10.1.1.1` (the primary TFTP server address) and click **OK**.

13. Click **OK** and **Commit** to save the configuration.

Configuring 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. 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 the DNS cache?	▶ *"Building Blocks of DNS Proxy"*
How do I configure static FQDN to IP address mappings?	▶ *"Building Blocks of DNS Proxy"*
What additional actions can I perform to manage DNS proxies?	▶ *"Additional DNS Proxy Actions"*

DNS Proxy Overview

▶ *Network > DNS Proxy*

To direct DNS queries to different DNS servers based on domain names you can configure the firewall as a DNS proxy and specify which DNS server(s) to use. 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.

You can also send DNS queries through a secure tunnel to protect details about the internal network configuration and enables you to use security features such as authentication and encryption.

For all DNS queries that are directed to an interface IP address, the firewall supports the selective directing of queries to different DNS servers based on full or partial domain names. TCP or UDP DNS queries are sent through the configured interface. UDP queries switch over to TCP when a DNS query answer is too long for a single UDP packet.

The interface includes the following tabs for defining DNS proxy:

- DNS Proxy Rules—Allows you to configure name, domain name, and primary and secondary DNS server settings.
- Static Entries—Allows you to configure static FQDN to IP address mappings that will be delivered in response to DNS queries made by hosts.
- Advanced—Allows you to define cache, TCP queries, and UDP Query Retries.

If the domain name is not found in the DNS proxy cache, the firewall searches for a match based on configuration of the entries in the specific DNS proxy object (on the interface on which the DNS query arrived) and forwards to a name server based on the match results. If no match is found, the default name servers are used. Static entries and caching are also supported.

▶ ***“Building Blocks of DNS Proxy”***

▶ ***“Moving or Cloning a Policy or Object”***

Building Blocks of DNS Proxy

▶ *Network > DNS Proxy*

The following section describes each component that you configure to set up the firewall as a DNS proxy.

Table 120. DNS Proxy Settings

Field	Configured In	Description
Enable	DNS Proxy	Select the check box to enable DNS proxy.
Name	DNS Proxy	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	DNS Proxy	Specify the virtual system to which the DNS proxy object applies. If you choose **Shared**, the **Server Profile** field is not available. Enter the **Primary** and **Secondary** DNS server IP addresses or address objects. For a virtual system to use DNS Proxy, you must configure one first. Go to **Device > Virtual Systems**, select a virtual system, and select a **DNS Proxy**.
Inheritance Source	DNS Proxy	Select a source 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	DNS Proxy	Click the link 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.
Server Profile	DNS Proxy	Select or create a new DNS server profile. This field does not appear if the Location of virtual systems was specified as Shared.
Primary Secondary	DNS Proxy	Specify the IP addresses of the default primary and secondary DNS servers. If the primary DNS server cannot be found, the secondary will be used.
Interface	DNS Proxy	Select the **Interface** check box to specify the firewall interfaces to support the DNS proxy rules. Select an interface from the drop-down list and click **Add**. You can add multiple interfaces. To delete an interface, select the interface and click **Delete**. An interface is not required if the DNS Proxy is used only for service route functionality. A destination service route should be used with a DNS proxy with no interface, if you want the source IP address to be set by the destination service route. Otherwise, the DNS proxy would select 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	DNS Proxy > DNS Proxy Rules	Select the check box to enable caching of domains that are resolved by this mapping.
Domain Name	DNS Proxy > DNS Proxy Rules	Click **Add** and enter the proxy server domain name. Repeat to add additional names. To delete a name, select the name and click **Delete**. For a DNS proxy rule, the number of tokens in a wildcard string must match the number of tokens in the requested domain. For example, "*.engineering.local" will not match "engineering.local". Both must be specified.
Primary/Secondary	DNS Proxy > DNS Proxy Rules	Enter the hostname or IP addresses of the primary and secondary DNS servers.
Name	DNS Proxy > Static Entries	Enter a name for the Static Entry.

Table 120. DNS Proxy Settings (Continued)

Field	Configured In	Description
FQDN	DNS Proxy > Static Entries	Enter the Fully Qualified Domain Name (FQDN) that will be mapped to the static IP addresses defined in the Address field.
Address	DNS Proxy > Static Entries	Click **Add** and enter the IP addresses that map to this domain. Repeat to add additional addresses. To delete an address, select the address and click **Delete**.
Cache	DNS Proxy > Advanced	Select the check box to enable DNS caching and specify the following information: • **Size**—Specify the number of entries that the cache will hold (range 1024-10240, default 1024). • **Timeout**—Specify the length of time (hours) after which all cached entries are removed. DNS time-to-live values are used to remove cache entries when they have been stored for less than the configured timeout period. Following a timeout, new requests must be resolved and cached again (range 4 to 24, default 4 hours).
TCP Queries	DNS Proxy > Advanced	Select the check box to enable DNS queries using TCP. Specify the upper limit on the number of concurrent pending TCP DNS requests that the firewall will support (range 64-256, default 64) in the **Max Pending Requests** field.
UDP Queries Retries	DNS Proxy > Advanced	Specify settings for UDP query retries: • **Interval**—Specify the time in seconds after which another request is sent if no response has been received (range 1-30, default 2 seconds). • **Attempts**—Specify the maximum number of attempts (excluding the first attempt) after which the next DNS server is tried (range 1-30, default 5).

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 deselect **Enable**. To enable a DNS proxy that is disabled, click into the name of the DNS proxy entry and select **Enable**.

Configuring 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"
How do I configure LLDP?	"Building Blocks of LLDP"
How do I configure an LLDP profile?	"Defining LLDP Profiles"
Looking for more?	**See** LLDP.

LLDP Overview

▶ ***Network > LLDP***

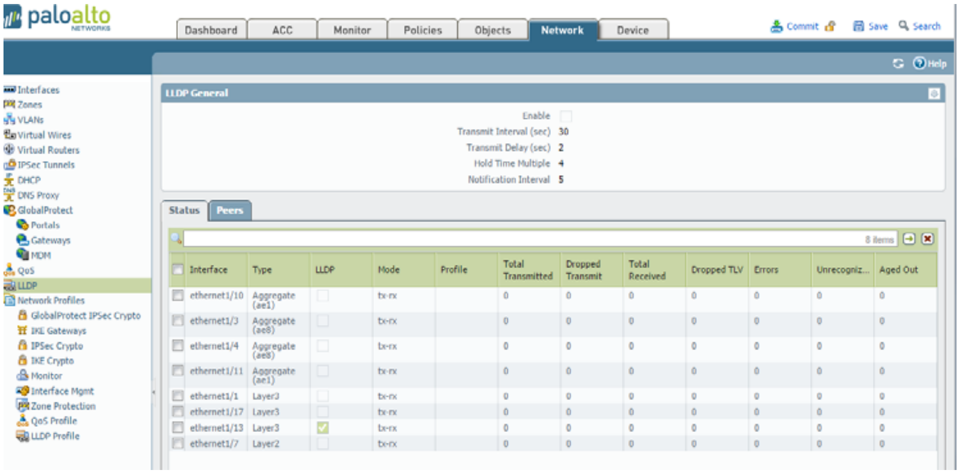
LLDP allows the firewall to send and receive Ethernet frames containing LLDP data units (LLDPDUs) to and from neighbors. The receiving device stores the information in a MIB, which can be accessed by the Simple Network Management Protocol (SNMP). LLDP enables network devices to map their network topology and learn capabilities of the connected devices. This makes troubleshooting easier, especially for virtual wire deployments where the firewall would typically go undetected in a network topology.

Building Blocks of LLDP

▶ ***Network > 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.

Table 121. LLDP Settings and Displayed Information



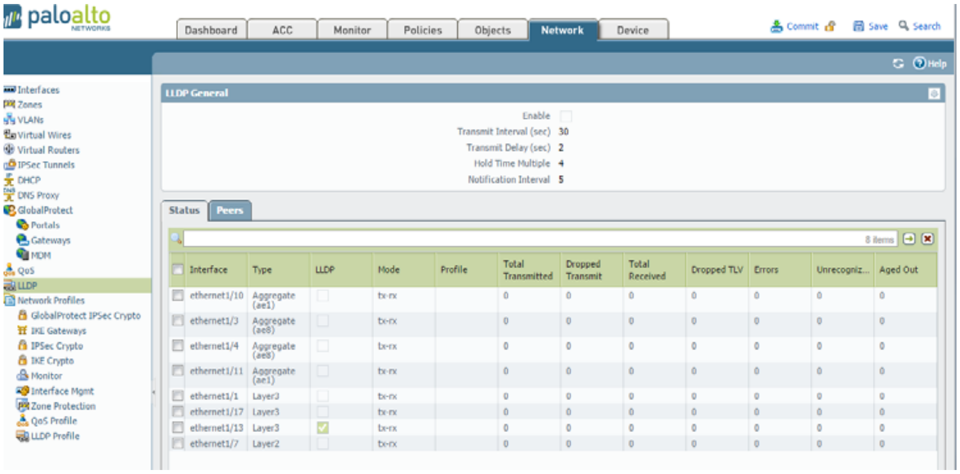
LLDP General

Enable □
Transmit Interval (sec) 30
Transmit Delay (sec) 2
Hold Time Multiple 4
Notification Interval 5

□	Interface	Type	LLDP	Mode	Profile	Total Transmitted	Dropped Transmit	Total Received	Dropped TLV	Errors	Unrecogniz...	Aged Out
□	ethernet1/10	Aggregate (ae1)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/3	Aggregate (ae8)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/4	Aggregate (ae8)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/11	Aggregate (ae1)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/1	Layer3	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/17	Layer3	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/13	Layer3	☑	tx-rx		0	0	0	0	0	0	0
□	ethernet1/7	Layer2	□	tx-rx		0	0	0	0	0	0	0

Field	Configured In or Displayed In	Description
Transmit Interval (sec)	LLDP	Specify the interval at which LLDPDUs are transmitted. Default: 30 seconds. Range: 1-3600 seconds.
Transmit Delay (sec)	LLDP	Specify the delay time 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**. Default: 2 seconds. Range: 1-600 seconds.
Hold Time Multiple	LLDP	Specify a value that is multiplied by the **Transmit Interval** to determine the total TTL hold time. The TTL hold time is the length of time the firewall will retain the information from the peer as valid. Default: 4. Range: 1-100. The maximum TTL hold time is 65535 seconds, regardless of the multiplier value.
Notification Interval	LLDP	Specify the interval at which syslog and SNMP Trap notifications are transmitted when MIB changes occur. Default: 5 seconds. Range: 1-3600 seconds.
spyglass filter	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	Status	Name of the interfaces that have LLDP profiles assigned to them.
LLDP	Status	LLDP status: enabled or disabled.
Mode	Status	LLDP mode of the interface: Tx/Rx, Tx Only, or Rx Only.
Profile	Status	Name of the profile assigned to the interface.
Total Transmitted	Status	Count of LLDPDUs transmitted out the interface.
Dropped Transmit	Status	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.

Table 121. LLDP Settings and Displayed Information (Continued)



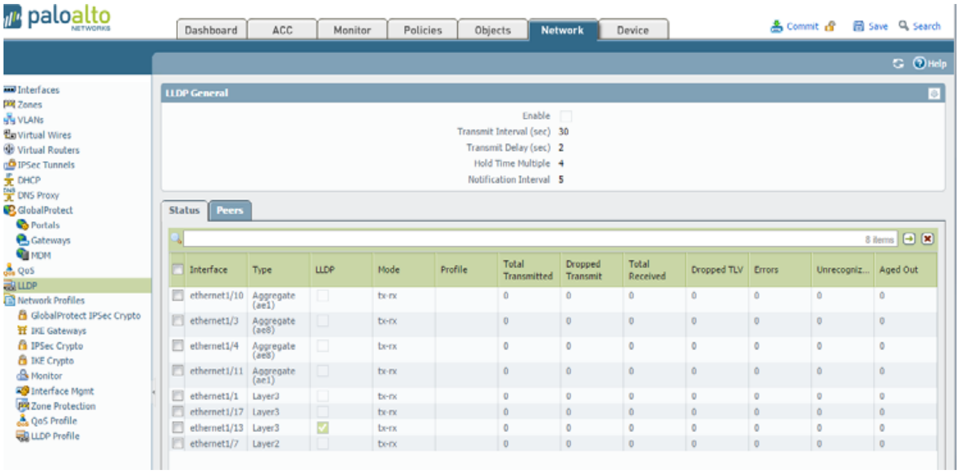
LLDP General

Enable □
Transmit Interval (sec) 30
Transmit Delay (sec) 2
Hold Time Multiple 4
Notification Interval 5

□	Interface	Type	LLDP	Mode	Profile	Total Transmitted	Dropped Transmit	Total Received	Dropped TLV	Errors	Unrecogniz...	Aged Out
□	ethernet1/10	Aggregate (ae1)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/3	Aggregate (ae8)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/4	Aggregate (ae8)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/11	Aggregate (ae1)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/1	Layer3	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/17	Layer3	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/13	Layer3	☑	tx-rx		0	0	0	0	0	0	0
□	ethernet1/7	Layer2	□	tx-rx		0	0	0	0	0	0	0

Field	Configured In or Displayed In	Description
Total Received	Status	Count of LLDP frames received on the interface.
Dropped TLV	Status	Count of LLDP frames discarded upon receipt.
Errors	Status	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	Status	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	Status	Count of items deleted from the Receive MIB due to proper TTL expiration.
Clear LLDP Statistics	Status	Click this button at the bottom of the screen to clear all of the LLDP statistics.
spyglass filter	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	Peers	Interface on the firewall that detected the neighboring device.
Remote Chassis ID	Peers	Chassis ID of the peer; the MAC address is used.
Port ID	Peers	Port ID of the peer.
Name	Peers	Name of the peer.
More Info	Peers	Click on this link to see Remote Peer Details, which are based on the Mandatory and Optional TLVs.
Chassis Type	Peers	Chassis Type is MAC address.
MAC Address	Peers	MAC address of the peer.
System Name	Peers	Name of the peer.
System Description	Peers	Description of the peer.

Table 121. LLDP Settings and Displayed Information (Continued)



LLDP General

Enable □
Transmit Interval (sec) 30
Transmit Delay (sec) 2
Hold Time Multiple 4
Notification Interval 5

□	Interface	Type	LLDP	Mode	Profile	Total Transmitted	Dropped Transmit	Total Received	Dropped TLV	Errors	Unrecogniz...	Aged Out
□	ethernet1/10	Aggregate (ae1)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/3	Aggregate (ae8)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/4	Aggregate (ae8)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/11	Aggregate (ae1)	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/1	Layer3	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/17	Layer3	□	tx-rx		0	0	0	0	0	0	0
□	ethernet1/13	Layer3	☑	tx-rx		0	0	0	0	0	0	0
□	ethernet1/7	Layer2	□	tx-rx		0	0	0	0	0	0	0

Field	Configured In or Displayed In	Description
Port Description	Peers	Port description of the peer.
Port Type	Peers	Interface name.
Port ID	Peers	Firewall uses the ifname of the interface.
System Capabilities	Peers	Capabilities of the system. O=Other, P=Repeater, B=Bridge, W=Wireless-LAN, R=Router, T=Telephone
Enabled Capabilities	Peers	Capabilities enabled on the peer.
Management Address	Peers	Management address of the peer.

Defining Interface Management Profiles

▶ *Network* > *Network Profiles* > *Interface Mgmt*

Use this page to specify the protocols that are used to manage the firewall. To assign management profiles to each interface, see “Configure a Layer 3 Interface” and “Configure a Layer 3 Subinterface”.

Table 122. Interface Management Profile Settings

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.
Ping Telnet SSH HTTP HTTP OCSP HTTPS SNMP Response Pages User-ID User-ID Syslog Listener-SSL User-ID Syslog Listener-UDP	Select the check box for each service you want to enable on the interfaces to which you assign the profile. If you select the **Response Pages** check box, the ports used to serve Captive Portal response pages are left open on Layer 3 interfaces: port 6080 for NTLM, 6081 for Captive Portal in transparent mode, and 6082 for Captive Portal in redirect mode. Selecting the **User-ID** check box enables communication between firewalls when one redistributes user mapping and group mapping information to the others. For details, see “User-ID Agents Tab”.
Permitted IP Addresses	Enter the list of IPv4 or IPv6 addresses from which firewall management is allowed.

Defining Monitor Profiles

▶ *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.

Table 123. **Monitor Settings**

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 2-10, default 3).
Threshold	Specify the number of heartbeats to be lost before the firewall takes the specified action (range 2-100, default 5).

Defining Zone Protection Profiles

▶ *Network > Network Profiles > Zone Protection*

A zone protection profile offers protection against most common floods, reconnaissance attacks and other packet-based attacks. It is designed to provide broad-based protection at the ingress zone (i.e. the zone where traffic enters the firewall) and are not designed to protect a specific end host or traffic going to a particular destination zone. To augment the zone protection capabilities on the firewall, use the DoS protection rulebase to match on a specific zone, interface, IP address or user.

Note: *Zone protection is only enforced when there is no session match for the packet. If the packet matches an existing session, it will bypass the zone protection setting.*

To configure a Zone Protection profile, click **Add** and specify the following settings:

Table 124. **Zone Protection Profile Settings**

Field	Description
Name	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.

When defining a Zone Protection profile you must configure the settings on the **General** tab and any of the following tabs as required by your network topology:

- **Flood Protection** tab: See “Configuring Flood Protection”.
- **Reconnaissance Profile** tab: See “Configuring Reconnaissance Protection”.
- **Packet Based Attack Protection** tab: See “Configuring Packet Based Attack 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, 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.

Configuring Flood Protection

▶ *Network > Network Profiles > Zone Protection > Flood Protection*

The following table describes the settings for the **Flood Protection** tab:

Table 125. Flood Protection tab Settings

Field	Description
Flood Protection Thresholds - SYN Flood	
Action	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, individual SYN packets are dropped randomly to restrict the flow. – When the flow exceeds the **Maximal** rate threshold, all packets are dropped. • **SYN Cookies**—Computes a sequence number for SYN-ACK packets that does not require pending connections to be stored in memory. This is the preferred method.
Alert (packets/sec)	Enter the number of SYN packets received by the zone (in a second) that triggers an attack alarm. Alarms can be viewed on the Dashboard (refer to "Using the Dashboard") and in the threat log (refer to "Taking Packet Captures").
Activate (packets/sec)	Enter the number of SYN packets received by the zone (in a second) that triggers the action specified.
Maximum (packets/sec)	Enter the maximum number of SYN packets able to be received per second. Any number of packets exceeding the maximum will be dropped.

Table 125. Flood Protection tab Settings (Continued)

Field	Description
Flood Protection Thresholds - ICMP Flood	
Alert (packets/sec)	Enter the number of ICMP echo requests (pings) received per second that triggers an attack alarm.
Activate (packets/sec)	Enter the number of ICMP packets received by the zone (in a second) that causes subsequent ICMP packets to be dropped.
Maximum (packets/sec)	Enter the maximum number of ICMP packets able to be received per second. Any number of packets exceeding the maximum will be dropped.
Flood Protection Thresholds - ICMPv6	
Alert (packets/sec)	Enter the number of ICMPv6 echo requests (pings) received per second that triggers an attack alarm.
Activate (packets/sec)	Enter the number of ICMPv6 packets received per second for the zone that causes subsequent ICMPv6 packets to be dropped. Metering stops when the number of ICMPv6 packets drops below the threshold
Maximum (packets/sec)	Enter the maximum number of ICMPv6 packets able to be received per second. Any number of packets exceeding the maximum will be dropped.
Flood Protection Thresholds - UDP	
Alert (packets/sec)	Enter the number of UDP packets received by the zone (in a second) that triggers an attack alarm.
Activate (packets/sec)	Enter the number of UDP packets received by the zone (in a second) that triggers random dropping of UDP packets. The response is disabled when the number of UDP packets drops below the threshold.
Maximum (packets/sec)	Enter the maximum number of UDP packets able to be received per second. Any number of packets exceeding the maximum will be dropped.
Flood Protection Thresholds - Other IP	
Alert (packets/sec)	Enter the number of IP packets received by the zone (in a second) that triggers an attack alarm.
Activate (packets/sec)	Enter the number of IP packets received by the zone (in a second) that triggers random dropping of IP packets. The response is disabled when the number of IP packets drops below the threshold. Any number of packets exceeding the maximum will be dropped.
Maximum (packets/sec)	Enter the maximum number of IP packets able to be received per second. Any number of packets exceeding the maximum will be dropped.

Configuring Reconnaissance Protection

▶ *Network > Network Profiles > Zone Protection > Reconnaissance Protection*

The following table describes the settings for the **Reconnaissance Protection** tab:

Table 126. Reconnaissance Protection tab Settings

Field	Description
Reconnaissance Protection - TCP Port Scan, UDP Port Scan, Host Sweep	
Interval (sec)	Enter the time interval for port scans and host sweep detection (seconds).
Threshold (events)	Enter the number of scanned ports within the specified time interval that will trigger this protection type (events).
Action	Enter the action that the system will take in response to this event type: • **Allow**—Permits the port scan of host sweep reconnaissance. • **Alert**—Generates an alert for each scan or sweep that matches the threshold within the specified time interval. • **Block**—Drops all further packets from the source to the destination for the remainder of the specified time interval. • **Block IP**—Drops all further packets for a specified period of time. Choose whether to block source, destination, or source-and-destination traffic and enter a duration (seconds).
IPv6 Drop Packets with	
Type 0 Router Header	Select the check box to drop IPv6 packets that include a Type 0 router header.
IPv4 Compatible Address	Select the check box to drop IPv6 packets that include an IPv4-compatible address.
Multicast Source Address	Select the check box to drop IPv6 packets that include a multicast source address.
Anycast Source Address	Select the check box to drop IPv6 packets that include an anycast source address.

Configuring Packet Based Attack Protection

▶ *Network > Network Profiles > Zone Protection > Packet Based Attack Protection*

The following tabs are used for configuration of Packet Based Attack protection:

- **IP Drop**: See “Configuring the IP Drop tab”.
- **TCP Drop**: See “Configuring the TCP Drop tab”.
- **ICMP Drop**: See “Configuring the ICMP Drop Tab”.
- **IPv6 Drop**: See “Configuring the IPv6 Drop Tab”.
- **ICMPv6**: See “Configuring the ICMPv6 Drop tab”.

Configuring the IP Drop tab

To configure IP Drop, specify the following settings:

Table 127. Packet Based Attack Protection tab Settings

Field	Description
IP Drop sub tab	

Table 127. Packet Based Attack Protection tab Settings (Continued)

Field	Description
Spoofed IP address	Select the check box to enable protection against IP address spoofing.
Strict IP Address Check	Select the checkbox to discard packets with malformed source or destination IP addresses. For example, discard packets where the source or destination IP address is the same as the network interface address, is a broadcast address, a loopback address, is a link-local address, is an unspecified address, or is reserved for future use. For a firewall in Common Criteria (CC) mode, you can also 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	Discards fragmented IP packets.
IP Option Drop	
Strict Source Routing	Discard packets with the Strict Source Routing IP option set.
Loose Source Routing	Discard packets with the Loose Source Routing IP option set.
Timestamp	Discard packets with the Timestamp IP option set.
Record Route	Discard packets with the Record Route IP option set.
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.
Malformed	Discard packets if they have incorrect combinations of class, number, and length based on RFC 791, 1108, 1393, and 2113.
Mismatched overlapping TCP segment	This setting will cause the firewall 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. • The segment covers another segment. This protection mechanism uses sequence numbers to determine where packets reside within the TCP data stream.
Remove TCP Timestamp	Determines whether the packet has a TCP timestamp in the header and, if it does, strips the timestamp from the header.
Reject Non-SYN TCP	Determines 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 the CLI. • **yes**—Reject non-SYN TCP. • **no**—Accept non-SYN TCP. Note that 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.
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 the CLI. • **drop**—Drop packets that contain an asymmetric path. • **bypass**—Bypass scanning on packets that contain an asymmetric path.

Configuring the TCP Drop tab

To configure TCP Drop, specify the following settings:

Table 128 TCP Drop tab Settings

Field	Description
Mismatched overlapping TCP segment	Causes the firewall 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. • The segment covers another segment. This protection mechanism uses sequence numbers to determine where packets reside within the TCP data stream.
Split Handshake	Prevents a TCP session from being established if the session establishment procedure does not use the well-known 3-way handshake. A 4-way or 5-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 option 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 3-way handshake; the variations are not allowed.
Reject Non-SYN TCP	Determines 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 the CLI. • **yes**—Reject non-SYN TCP. • **no**—Accept non-SYN TCP. Note that 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.
Asymmetric Path	Determines 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 the CLI. • **drop**—Drop packets that contain an asymmetric path. • **bypass**—Bypass scanning on packets that contain an asymmetric path.
Remove TCP Timestamp	Determines whether the packet has a TCP timestamp in the header and, if it does, strips the timestamp from the header.

Configuring the ICMP Drop Tab

To configure ICMP Drop, specify the following settings:

Table 129. ICMP Drop tab Settings

Field	Description
ICMP Drop sub tab	
ICMP Ping ID 0	Discards packets if the ICMP ping packet has an identifier value of 0.
ICMP Fragment	Discards packets that consist of ICMP fragments.

Table 129. ICMP Drop tab Settings (Continued)

Field	Description
ICMP Large Packet (>1024)	Discards ICMP packets that are larger than 1024 bytes.
Discard ICMP embedded with error message	Discards ICMP packets that are embedded with an error message.
Suppress ICMP TTL Expired Error	Stops sending ICMP TTL expired messages.
Suppress ICMP Frag Needed	Stops 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.

Configuring the IPv6 Drop Tab

To configure IPv6 Drop, specify the following settings:

Table 130. IPv6 Drop tab Settings

Field	Description
IPv6 Drop sub tab	
Type 0 Routing Heading	Discards IPv6 packets containing a Type 0 routing header. See RFC 5095 for Type 0 routing header information.
IPv4 compatible address	Discards IPv6 packets that are defined as an RFC 4291 IPv4-Compatible IPv6 address.
Anycast source address	Discards IPv6 packets that contain an anycast source address.
Needless fragment header	Discards IPv6 packets with the last fragment flag (M=0) and offset of zero.
MTU in ICMP 'Packet Too Big' less than 1280 bytes	Discards IPv6 packets that contain a Packet Too Big ICMPv6 message when the maximum transmission unit (MTU) is less than 1280 bytes.
Hop-by-Hop extension	Discards IPv6 packets that contain the Hop-by-Hop Options extension header.
Routing extension	Discards 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	Discards 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	Discards IPv6 packets that contain invalid IPv6 options in an extension header.
Non-zero reserved field	Discards IPv6 packets that have a header with a reserved field not set to zero.

Configuring the ICMPv6 Drop tab

To configure ICMPv6 Drop, specify the following settings:

Table 131. ICMPv6 Drop tab Settings

Field	Description
ICMPv6 sub tab	
ICMPv6 destination unreachable - require explicit security rule match	Require an explicit security policy match for destination unreachable ICMPv6 errors even when 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 errors even when associated with an existing session.
ICMPv6 time exceeded - require explicit security rule match	Require an explicit security policy match for time exceeded ICMPv6 errors even when associated with an existing session.
ICMPv6 parameter problem - require explicit security rule match	Require an explicit security policy match for parameter problem ICMPv6 errors even when associated with an existing session.
ICMPv6 redirect - require explicit security rule match	Require an explicit security policy match for redirect ICMPv6 messages even when associated with an existing session.

Defining LLDP Profiles

What are you looking for?	See
What is LLDP?	“LLDP Overview”
How do I configure LLDP?	“Building Blocks of LLDP”
How do I configure an LLDP profile?	“Building Blocks of LLDP Profiles”
Looking for more?	**See** LLDP.

Building Blocks of LLDP Profiles

▶ *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.

Table 132. LLDP Profile Settings

Field	Configured In	Description
Name	LLDP Profile	Specify a name for the LLDP profile.
Mode	LLDP Profile	Select the mode in which LLDP will function: **transmit-receive**, **transmit-only**, or **receive-only**.
SNMP Syslog Notification	LLDP Profile	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**.
Port Description	LLDP Profile	Enables the ifAlias object of the firewall to be sent in the Port Description TLV.
System Name	LLDP Profile	Enables the sysName object of the firewall to be sent in the System Name TLV.
System Description	LLDP Profile	Enables the sysDescr object of the firewall to be sent in the System Description TLV.
System Capabilities	LLDP Profile	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	LLDP Profile	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, use the **Move Up** or **Move Down** buttons.
Name	LLDP Profile	Specify a name for the Management Address.
Interface	LLDP Profile	Select an interface whose IP address will be the Management Address. If **None** is specified, you can enter an IP address in the field next to the IPv4 or IPv6 selection.
IP Choice	LLDP Profile	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.

Chapter 5

Policies and Security Profiles

This section describes how to configure policies and security profiles:

- "Policy Types"
- "Moving or Cloning a Policy or Object"
- "Security Profiles"
- "Other Policy Objects"

Policy Types

Policies allow you to control firewall operation by enforcing rules and automatically taking action. The following types of policies are supported:

Basic security policies to block or allow a network session based on the application, the source and destination zones and addresses, and optionally the service (port and protocol). Zones identify the physical or logical interfaces that send or receive the traffic. Refer to "Defining Security Policies".

For information on using the tag browser, see "Use the Tag Browser".

- Network Address Translation (NAT) policies to translate addresses and ports, as needed. Refer to "NAT Policies" and "Defining Network Address Translation Policies".
- Policy-based forwarding policies to override the routing table and specify an egress interface for traffic. Refer to "Policy-Based Forwarding Policies".
- 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. Refer to "Decryption Policies".
- Override policies to override the application definitions provided by the firewall. Refer to "Defining Application Override Policies".
- Quality of Service (QoS) policies to determine how traffic is classified for treatment when it passes through an interface with QoS enabled. Refer to "QoS Statistics".

- Captive portal policies to request authentication of unidentified users. Refer to "Defining Captive Portal Policies".
- Denial of service (DoS) policies to protect against DoS attacks and take protective action in response to rule matches. Refer to "Defining DoS Policies".

Shared polices pushed from Panorama™ display in green on the firewall web interface; these shared policies cannot be edited on the firewall.

Moving or Cloning a Policy or Object

When moving or cloning policies and 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 policies or objects, select them in the **Policies** or **Objects** tab, click **Move**, select **Move to other vsys** (firewalls only) or **Move to other device group** (Panorama only), complete the fields in the following table, and then click **OK**.

To clone policies or objects, select them in the **Policies** or **Objects** tab, click **Clone**, complete the fields in the following table, and then click **OK**.

Table 133 Move/Clone Settings

Field	Description
Selected Rules/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.
Rule order (policies only)	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 check box (selected by default) to make the device 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 the check box, the device will find all the errors before displaying them.

Overriding or Reverting a Default Security 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 device 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 "Defining Security Policies".

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.

Table 134 Override a Default Security Rule

Field	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.
Description	The **Description** is read-only; you cannot override it.
Tag	Select a tag 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 datacenter for policies associated with that location.
Actions Tab	
Action Setting	**Action**: Select one of the following actions 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 individual **Antivirus**, **Vulnerability Protection**, **Anti-Spyware**, **URL Filtering**, **File Blocking**, **Data Filtering**, and/or **WildFire Analysis** 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 (see “Security Profiles”) or profile groups (see “Security Profile Groups”), click **New** in the drop-down for the corresponding profile or group.

Table 134 Override a Default Security Rule (Continued)

Field	Description
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 "Log Forwarding"). • To generate entries in the local traffic log for traffic that matches this rule, select the following options: – **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). **Note:** *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.*

Overriding or Reverting 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 it 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.

To 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 the object **Name** or **Shared** settings.

To 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.

To 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 the **Disable override** check box, and click **OK**. Overrides for that object are then disabled in all descendants of the selected **Device Group**.

To 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 the **Ancestor Objects Take Precedence** check box, and click **OK**. You must then commit to Panorama and to the device groups containing overrides to push the inherited values.

Specifying Users and Applications for Policies

▶ *Policies > Security*

▶ *Policies > Decryption*

You can restrict security policies to be applied to selected users or applications by clicking the **User** or **Application** link on the **Security** or **Decryption** device rules page. For information on restricting rules by application, refer to “Defining Applications”.

To restrict a policy to selected users/groups, follow these steps:

1. On the **Security** or **Decryption** device rules page, click the **User** tab to open the selection window.

> *If you are using a RADIUS server and not the User-ID™ Agent, the list of users is not displayed, and you must enter user information manually.*

2. Click the drop-down menu above the **Source User** table to select the user type:
   - **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 clients, 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 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.
3. To add groups of users, select from the **Available User Groups** check boxes and click **Add User Group**. Alternatively, you can enter text to match one or more groups and click **Add User Group**.
4. To add individual users, enter a search string in the **User** search field and click **Find**. You can then select users and click **Add User**. Alternatively, you can enter individual user names in the **Additional Users** area.
5. Click **OK** to save the selections and update the security or decryption rule.

Defining Policies on Panorama

Device Groups on Panorama allow you to centrally manage policies on the managed devices (or firewalls). Policies defined on Panorama are either created as **Pre Rules** or as **Post Rules**; Pre Rules and Post Rules allow you to create a layered approach in implementing policy.

Pre rules and Post rules can be defined in a shared context as shared policies for all managed devices, or in a device group context to make it specific to a device group. Because Pre rules and Post Rules are defined on Panorama and then pushed from Panorama to the managed devices, you can view the rules on the managed firewalls, but can only edit the Pre Rules and Post Rules 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, to block access to specific URL categories, or to 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 the rules locally defined on the device. Post-rules typically include rules to deny access to traffic based on the App-ID™, User-ID, or Service.
- **Default Rules**—Rules that instruct the firewall how to handle traffic that does not match any Pre Rules, Post Rules, or local device rules. These rules are part of Panorama's predefined configuration. You must **Override** them to enable editing of select settings in these rules: see "Overriding or Reverting a Default Security Rule".

Use **Preview Rules** to view a list of the rules before you push the rules to the managed devices. Within each rulebase, the hierarchy of rules is visually demarcated for each device group (and managed device) to make it easier to scan through a large numbers of rules.

To create policies, see the relevant section for each rulebase:

- "Defining Security Policies"
- "Defining Network Address Translation Policies"
- "QoS Statistics"
- "Policy-Based Forwarding Policies"
- "Decryption Policies"
- "Defining Application Override Policies"
- "Defining Captive Portal Policies"
- "Defining DoS Policies"

Defining Security Policies

▶ ***Policies > Security***

Security policies 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 Policies Overview"*** ▶ ***For Panorama, see "Defining Policies on Panorama"***
What are the fields available to create a security policy?	▶ ***"Building Blocks in a Security Policy"***
How can I use the web interface to manage security policies?	▶ ***"Creating and Managing Policies"***
Do you want more? Can't find what you're looking for?	**See** Security Policy

Security Policies Overview

▶ *Policies > Security*

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.

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 pre-defined 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.

- **General**—Use the **General** tab to configure a name and description for the security policy.
- **Source**—Use the **Source** tab to define the source zone or source address from which the traffic originates.
- **User**—Use 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**—Use the **Destination** tab to define the destination zone or destination address for the traffic.
- **Application**—Use 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**—Use 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.
- **Action**—Use the **Action** tab to determine the action that will be taken based on traffic that matches the defined policy attributes.

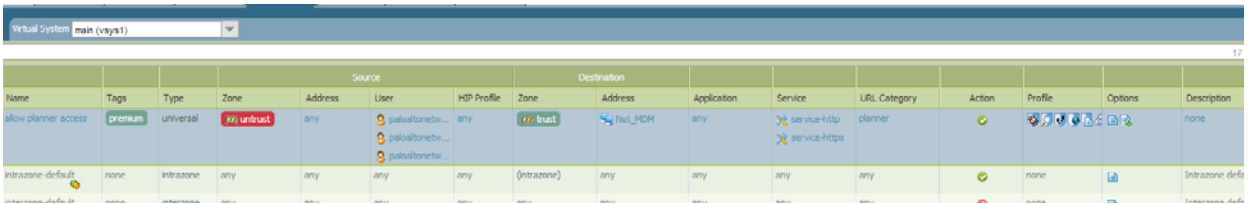
See:

- ▶ *"Building Blocks in a Security Policy"*
- ▶ *"Creating and Managing Policies"*

Building Blocks in a Security Policy

The following section describes each building block or component in a security policy rule. When you view the default security rule, or create a new rule, you can configure the options described here.

Table 135. Building Blocks in a Security Rule



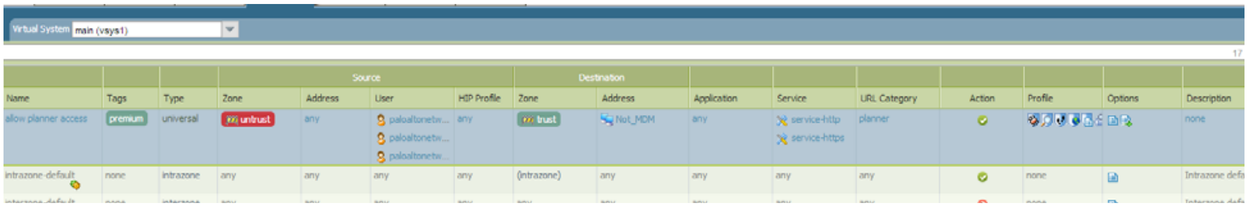
Virtual System main (vsys1)

17

			Source				Destination								
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Description
allow planner access	premium	universal	untrust	any	paloaltonetw... paloaltonetw... paloaltonetw...	any	trust	Not_MDM	any	service-http service-https	planner	✓			none
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	✓	none		Intrazone defa
interzone-default	none	interzone	any	any	any	any	any	any	any	any	any		none		Interzone defa

Field	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 filter(s), each rule is listed with its number in the context of the complete set of rules in the rulebase and its place in the evaluation order. In Panorama, pre-rules and post-rules are independently numbered. When rules are pushed from Panorama to a managed firewall, the rule numbering incorporates hierarchy in pre-rules, device 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 31 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.
Tag	**General**	Click **Add** to 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.

Table 135. Building Blocks in a Security Rule



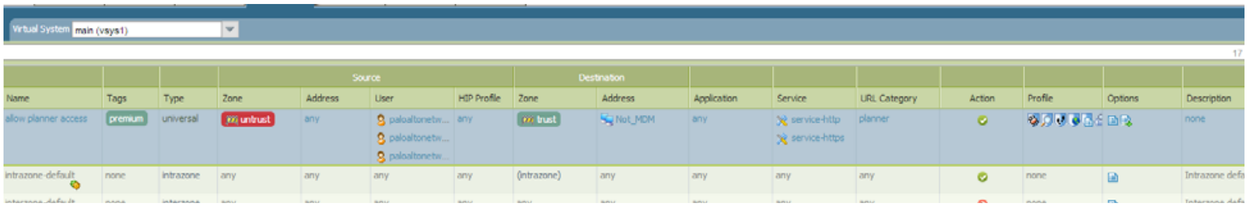
Virtual System main (vsys1)

17

			Source				Destination								
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Description
allow planner access	premium	universal	untrust	any	paloaltonetw... paloaltonetw... paloaltonetw...	any	trust	Not_MDM	any	service-http service-https	planner	✓			none
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	✓	none		Intrazone defa
interzone-default	none	interzone	any	any	any	any	any	any	any	any	any		none		Interzone defa

Field	Configured In	Description
Type	**General**	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 role 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 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.
Source Zone	**Source**	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 "Defining Security 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**	Click **Add** to add source addresses, address groups, or regions (default is any). Select from the drop-down list, or click the **Address**, **Address Group**, or **Regions** at the bottom of the drop-down list, and specify the settings.

Table 135. Building Blocks in a Security Rule



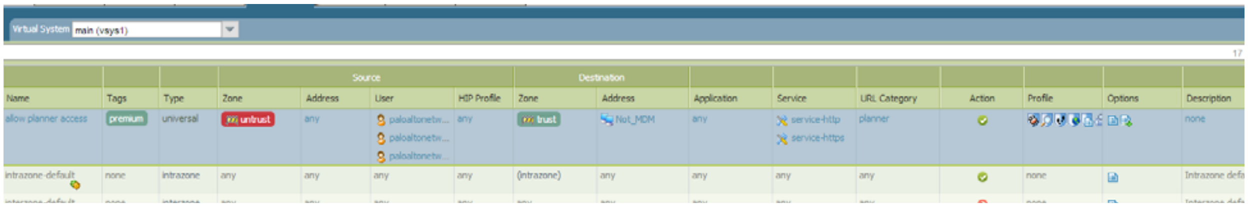
Virtual System main (vsys1)

17

			Source				Destination								
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Description
allow planner access	premium	universal	untrust	any	paloaltonetw... paloaltonetw... paloaltonetw...	any	trust	Not_MDM	any	service-http service-https	planner	✓			none
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	✓	none		Intrazone defa
interzone-default	none	interzone	any	any	any	any	any	any	any	any	any		none		Interzone defa

Field	Configured In	Description
Source User	**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 clients, 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 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. **Note:** *If you are using a RADIUS server and not the User-ID agent, the list of users is not displayed, and you must enter user information manually.*
Source HIP Profile	**User**	Click **Add** to choose host information profiles (HIP) to identify users. A HIP enables 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 access to your network resources.

Table 135. Building Blocks in a Security Rule



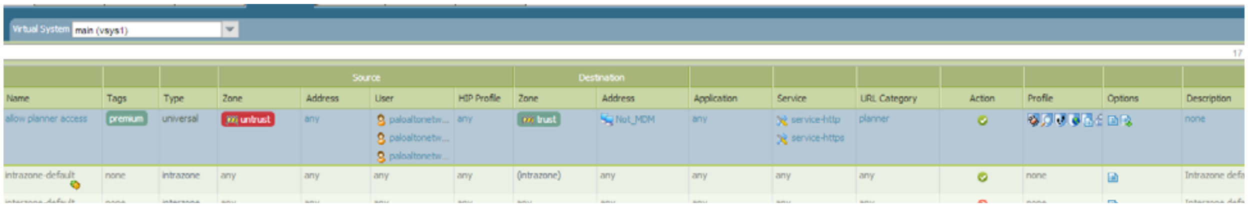
Virtual System main (vsys1)

17

			Source				Destination								
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Description
allow planner access	premium	universal	untrust	any	paloaltonetw... paloaltonetw... paloaltonetw...	any	trust	Not_MDM	any	service-http service-https	planner	✓			none
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	✓	none		Intrazone defa

Field	Configured In	Description
Destination Zone	**Destination**	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 “Defining Security 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. **Note:** *On intrazone rules, you cannot define a Destination Zone because these types of rules only match traffic with a source and a destination within the same zone. To specify the zones that match an intrazone rule you only need to set the Source Zone.*
Destination Address	**Destination**	Click **Add** to add destination addresses, address groups, or regions (default is **any**). Select from the drop-down list, or click the **Address** link at the bottom of the drop-down list, and specify address settings.
Application	**Application**	Select specific applications for the security 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 rule, you can view details of these objects by holding your mouse over the object in the **Application** column, click the drop-down arrow and select **Value**. This allows you to easily view application members directly from the policy without having to navigate to the **Object** tabs.

Table 135. Building Blocks in a Security Rule

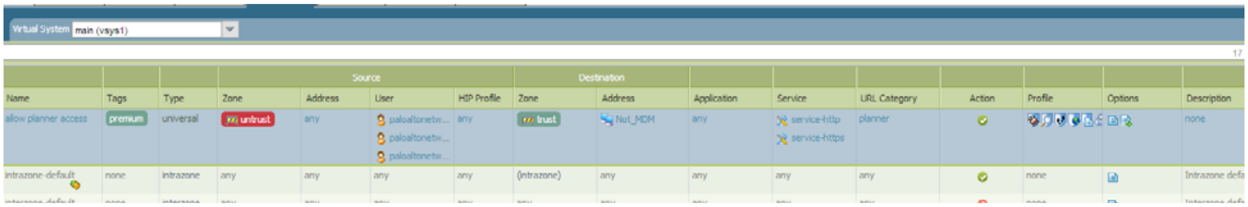


Virtual System main (vsys1)

			Source				Destination								
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Description
allow planner access	premium	universal	untrust	any	paloaltonetw... paloaltonetw... paloaltonetw...	any	trust	Not_MDM	any	service-http service-https	planner	✓			none
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	✓	none		Intrazone defa

Field	Configured In	Description
Service	**Service/URL Category**	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 because it prevents applications from running on unusual ports and protocol which, if not intentional, can be a sign of undesired application behavior and usage. Note that when you use this option, the device still checks for all applications on all ports but, with this configuration, applications are only allowed on their default ports and protocols. • **Select**—Click **Add**. Choose an existing service or choose **Service** or **Service Group** to specify a new entry. Refer to "Services" and "Service Groups".
URL Category	**Service/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, click **Add** and select a specific category (including a custom category) from the drop-down. You can add multiple categories. Refer to "Dynamic Block Lists" for information on defining custom categories.

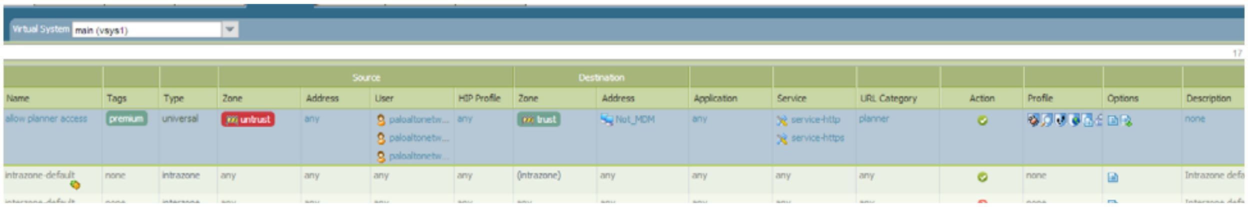
Table 135. Building Blocks in a Security Rule



			Source				Destination								
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Description
allow planner access	premium	universal	untrust	any	paloaltonetw... paloaltonetw... paloaltonetw...	any	trust	Not_MDM	any	service-http service-https	planner	✓			none
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	✓	none		Intrazone defa

Field	Configured In	Description
Action	**Actions**	To specify the action for traffic that matches the attributes defined in a rule, select from the following actions: – **Allow**—(default) Allows the traffic. – **Deny**—Blocks traffic, and enforces the default *Deny Action* defined for the application that is being denied. To view the deny action defined by default for an application, view the application details in **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 could drop the session silently for another application. – **Drop**—Silently drops the application. A TCP reset is not sent to the host/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**—Sends a TCP reset to both the client-side and server-side devices. • **Send ICMP Unreachable**- Only available for Layer 3 interfaces. When you configure security policy 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 the Session Settings section in **Device > Setup > Session**. To override the default action defined on the predefined interzone and intrazone rules: see “Overriding or Reverting a Default Security Rule”

Table 135. Building Blocks in a Security Rule

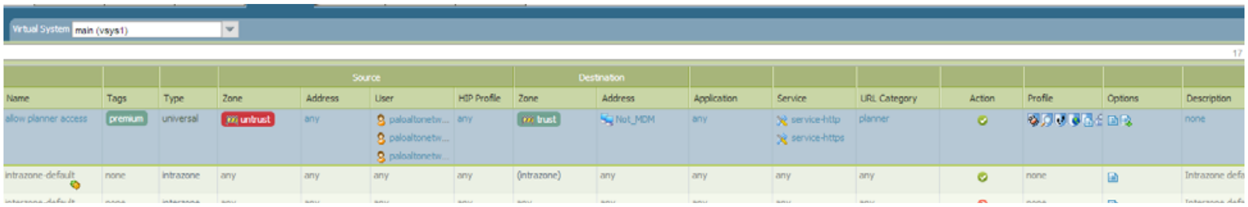


Virtual System main (vsys1)

			Source				Destination								
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Description
allow planner access	premium	universal	untrust	any	paloaltonetw... paloaltonetw... paloaltonetw...	any	trust	Not_MDM	any	service-http service-https	planner	✓			none
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	✓	none		Intrazone defa

Field	Configured In	Description
Profile Setting	**Actions**	To specify the checking done by the default security profiles, select individual Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, and/or Data Filtering profiles. To specify a profile group rather than individual profiles, select **Profile Type Group** and then select a profile group from the **Group Profile** drop-down. To define new profiles or profile groups, click **New** next to the appropriate profile or group (refer to “Security Profile Groups”). You can also attach security profiles (or profile groups) to the default rules.

Table 135. Building Blocks in a Security Rule



Virtual System main (vsys1)

17

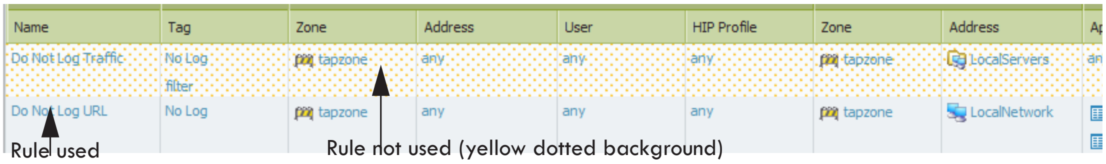
			Source				Destination								
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Description
allow planner access	premium	universal	untrust	any	paloaltonetw... paloaltonetw... paloaltonetw...	any	trust	Not_MDM	any	service-http service-https	planner	✓			none
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	✓	none		Intrazone defa

Field	Configured In	Description
Options	**Actions**	The **Options** tab includes the logging settings and the a combination of other options listed below: To generate entries in the local traffic log for traffic that matches this rule, select the following options: • **Log At Session Start**. Generates a traffic log entry for the start of a session (disabled by default). • **Log At Session End**. Generates a traffic log entry for the end of a session (enabled by default). Note: 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 profile from the **Log Forwarding Profile** drop-down. Note that the generation of threat log entries is determined by the security profiles. To define new log profiles, click **New** (refer to “Log Forwarding”). 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. To define new schedules, click **New** (refer to “SSL Decryption Settings in a Decryption Profile”). • **QoS Marking**—To change the Quality of Service (QoS) setting on packets matching the rule, select IP DSCP or IP Precedence and enter the QoS value in binary or select a predefined value from the drop-down. For more information on QoS, refer to “Configuring Quality of Service”. • **Disable Server Response Inspection—**To disable packet inspection from the server to the client, select this check box. This option may be useful under heavy server load conditions.
Description	**General**	Enter a description for the policy (up to 255 characters).

Creating and Managing Policies

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

Task	Description
Add	To add a new policy rule, do one of the following: • Click **Add** at the bottom of the page. • Select a rule on which to base the new rule and click **Clone Rule**, or select a rule by clicking the white space of the rule and select **Clone Rule** at the bottom of the page (a rule that is selected in the web interface displays with a yellow background). 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 "Moving or Cloning a Policy or Object".
Modify	To modify a rule, click the rule. If the rule is pushed from Panorama, the rule is read-only on the firewall and cannot be edited locally. **Override** and **Revert** actions only pertain to the default rules that are displayed at the bottom of the Security rulebase. These predefined rules—allow all intrazone traffic and deny all interzone traffic—instruct the firewall on 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 in order 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 Default Security Rule".
Move	Rules are evaluated top down and as enumerated on the **Policies** page. To change the order in which the rules are evaluated against network traffic, select a rule and click **Move Up**, **Move Down**, **Move Top**, or **Move Bottom.** For details, see "Moving or Cloning a Policy or Object".
Delete	Select a rule and click **Delete** to remove the existing rule.
Enable/ Disable	To disable a rule, select the rule and click **Disable**. To enable a rule that is disabled, select the rule and click **Enable**.
View Unused rules	To find currently unused rules, select the **Highlight Unused Rules** check box. You can then decide whether to disable the rule or delete it. The rules are not currently used display with a dotted yellow background. **Best Practice**: Each device maintains a flag for the rules that have a match. Because the flag is reset when a dataplane reset occurs on a reboot or a restart, monitor this list periodically to determine whether the rule has had a match since the last check before you delete or disable it.



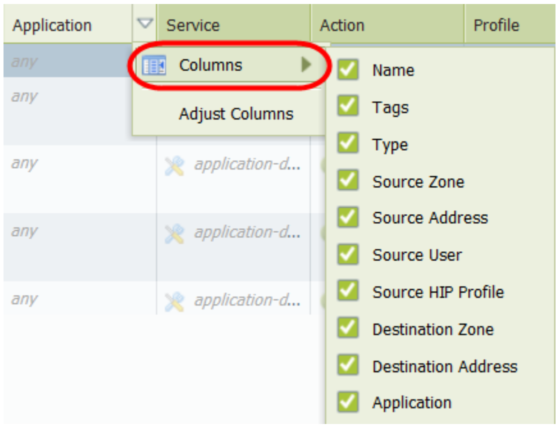
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Ap
Do Not Log Traffic	No Log filter	tapzone	any	any	any	tapzone	LocalServers	an
Do Not Log URL	No Log	tapzone	any	any	any	tapzone	LocalNetwork	

Rule used

Rule not used (yellow dotted background)

<table>
<tr><th>Task</th><th>Description</th></tr>
<tr><td>Show/Hide columns</td><td>

To change (show or hide) the columns that display in any of the <b>Policies</b> pages. Select or clear the check box next to the column name to toggle the display for each column.

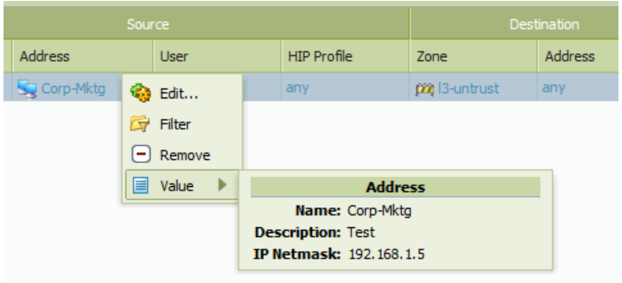


</td></tr>
<tr><td>Apply filters</td><td>

To apply a filter to the list, select from the <b>Filter Rules</b> drop-down. To add a value to define a filter, click the drop-down for the item and choose <b>Filter</b>. <b>Note</b>: The default rules are not part of rulebase filtering and always show up in the list of filtered rules.

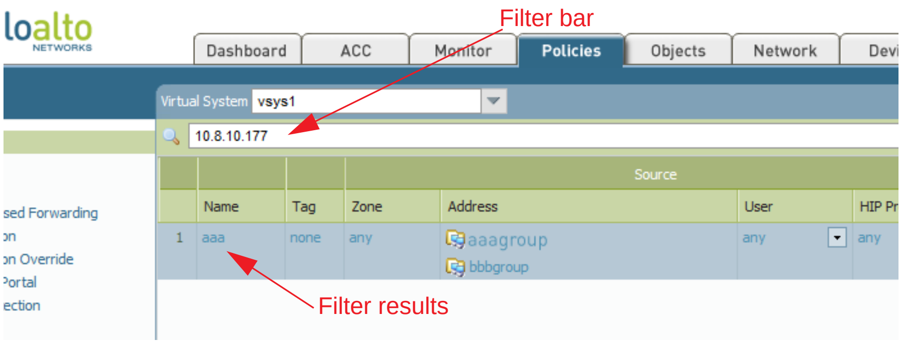
To view the network sessions that were logged as matches against the policy, click the drop-down for the rule name and choose <b>Log Viewer.</b>

To display the current value by clicking the drop-down for the entry and choosing <b>Value</b>. You can also edit, filter, or remove certain items directly from the column menu. For example, to view addresses included in an address group, hold your mouse over the object in the <b>Address</b> column, click the drop-down and select <b>Value</b>. This allows you to quickly view the members and the corresponding IP addresses for the address group without having to navigate to the <b>Object</b> tabs.



<b>Address</b>
<b>Name:</b> Corp-Mktg
<b>Description:</b> Test
<b>IP Netmask:</b> 192.168.1.5

</td></tr>
</table>

Task	Description
	To find objects that are used within a policy based on the object name or IP address, use the filter. The search will comb through embedded objects to find an address within an address object or address group. In the following screen shot, the IP address 10.8.10.177 was entered in the filter bar and the aaa policy is shown. That policy uses an address group object named aaagroup, which contains the IP address.  Filter bar Dashboard ACC Monitor Policies Objects Network Devi sed Forwarding on on Override Portal ection Filter results Virtual System: vsys1 10.8.10.177 Source: Name: aaa; Tag: none; Zone: any; Address: aaagroup, bbbgroup; User: any; HIP Pr: any
Preview rules (Panorama only)	Use **Preview Rules** to view a list of the rules before you push the rules to the managed devices. Within each rulebase, the hierarchy of rules is visually demarcated for each device group (and managed device) to make it easier to scan through a large numbers of rules.

NAT Policies

If you define Layer 3 interfaces on the firewall, you can use Network Address Translation (NAT) policies 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. When performing NAT on virtual wire interfaces, it is recommended that you translate the source address to a different subnet than the one on which the neighboring devices are communicating. Proxy ARP is not supported on virtual wires, so neighboring devices will only be able to resolve ARP requests for IP addresses that reside on the interface of the device on the other end of the virtual wire.

When configuring NAT on the firewall, it is important to note that a security policy must also be configured to allow the NAT traffic. Security policy will be matched based on the post-NAT zone and the pre-NAT IP address.

The firewall supports the following types of address translation:

- **Dynamic IP/Port**—For outbound traffic. Multiple clients can use the same public IP addresses with different source port numbers. Dynamic IP/Port NAT rules allow translation to a single IP address, a range of IP addresses, a subnet, or a combination of these. In cases where an egress interface has a dynamically assigned IP address, it can be helpful to specify the interface itself as the translated address. By specifying the interface in the dynamic IP/port rule, NAT policy will update automatically to use any address acquired by the interface for subsequent translations.

Palo Alto Networks Dynamic IP/port NAT supports more NAT sessions than are supported by the number of available IP addresses and ports. The firewall can use IP address and port combinations up to two times (simultaneously) on the PA-200, PA-500, PA-2000 Series and PA-3000 Series firewalls, four times on the PA-4020 and PA-5020 firewalls, and eight times on the PA-4050, PA-4060, PA-5050, PA-5060, and PA-7000 Series firewalls when destination IP addresses are unique.

- **Dynamic IP**—For outbound traffic. Private source addresses translate to the next available address in the specified address range. Dynamic IP NAT policies allow you to specify a single IP address, multiple IPs, multiple IP ranges, or multiple subnets as the translated address pool. If the source address pool is larger than the translated address pool, new IP addresses seeking translation will be blocked while the translated address pool is fully utilized. To avoid this issue, you can specify a fall back pool that will be used if the primary pool runs out of IP addresses.

- **Static IP**—For inbound or outbound traffic. You can use static IP to change the source or the destination IP address while leaving the source or destination port unchanged. When used to map a single public IP address to multiple private servers and services, destination ports can stay the same or be directed to different destination ports.

You may need to define static routes on the adjacent router and/or the firewall to ensure that traffic sent to a public IP address is routed to the appropriate private address. If the public address is the same as the firewall interface (or on the same subnet), then a static route is not required on the router for that address. When you specify service (TCP or UDP) ports for NAT, the pre-defined HTTP service (service-http) includes two TCP ports: 80 and 8080. To specify a single port, such as TCP 80, you must define a new service.

The next table summarizes the NAT types. The two dynamic methods map a range of client addresses (M) to a pool (N) of NAT addresses, where M and N are different numbers. N can also be 1. Dynamic IP/Port NAT differs from Dynamic IP NAT in that the TCP and UDP source ports are not preserved in Dynamic IP/Port, whereas they are unchanged with Dynamic IP NAT. There are also differing limits to the size of the translated IP pool, as noted below.

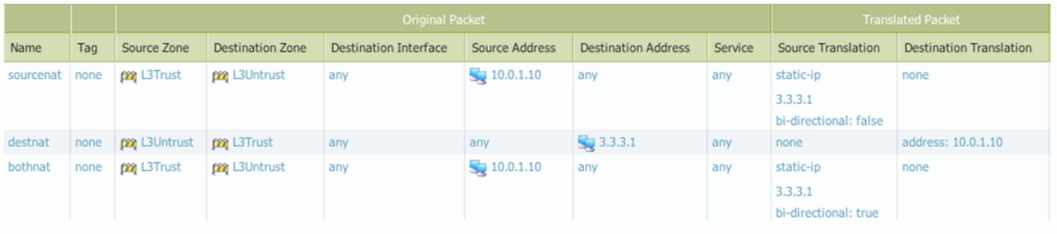
With Static IP NAT, there is a one-to-one mapping between each original address and its translated address. This can be expressed as 1-to-1 for a single mapped IP address, or M-to-M for a pool of many one-to-one, mapped IP addresses.

Table 136. NAT Types

PAN-OS NAT Type	Source Port Stays the Same	Destination Port Can Change	Mapping Type	Size of Translated Address Pool
Dynamic IP/ Port	No	No	Many-to-1 M-to-N	Up to 254 consecutive addresses
Dynamic IP	Yes	No	M-to-N	Up to 32k consecutive addresses

Table 136. NAT Types (Continued)

PAN-OS NAT Type	Source Port Stays the Same	Destination Port Can Change	Mapping Type	Size of Translated Address Pool
Static IP	Yes	No	1-to-1 M-to-M MIP	Unlimited
	Optional		1-to-Many VIP PAT	



		Original Packet						Translated Packet	
Name	Tag	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
sourcenat	none	L3Trust	L3Untrust	any	10.0.1.10	any	any	static-ip 3.3.3.1 bi-directional: false	none
destnat	none	L3Untrust	L3Trust	any	any	3.3.3.1	any	none	address: 10.0.1.10
bothnat	none	L3Trust	L3Untrust	any	10.0.1.10	any	any	static-ip 3.3.3.1 bi-directional: true	none

Determining Zone Configuration in NAT and Security Policy

NAT rules must be configured to use the zones associated with pre-NAT IP addresses configured in the policy. For example, if you are translating traffic that is incoming to an internal server (which is reached via a public IP by Internet users), it is necessary to configure the NAT policy using the zone in which the public IP address resides. In this case, the source and destination zones would be the same. As another example, when translating outgoing host traffic to a public IP address, it is necessary to configure NAT policy with a source zone corresponding to the private IP addresses of those hosts. The pre-NAT zone is required because this match occurs before the packet has been modified by NAT.

Security policy differs from NAT policy in that post-NAT zones must be used to control traffic. NAT may influence the source or destination IP addresses and can potentially modify the outgoing interface and zone. When creating security policies with specific IP addresses, it is important to note that pre-NAT IP addresses will be used in the policy match. Traffic subject to NAT must be explicitly permitted by the security policy when that traffic traverses multiple zones.

NAT Rule Options

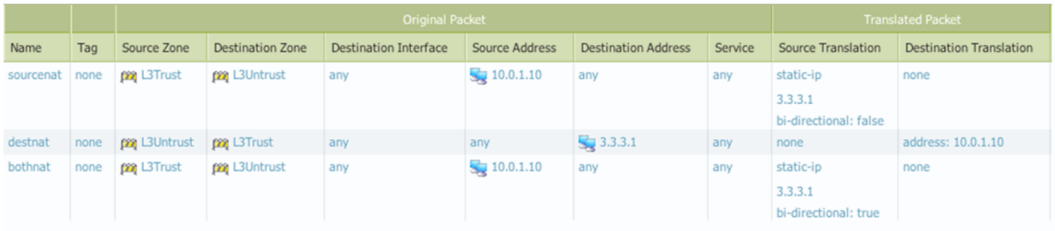
The firewall supports no-NAT rules and bi-directional NAT rules.

No-NAT Rules

No-NAT rules are configured to allow exclusion of IP addresses defined within the range of NAT rules defined later in the NAT policy. To define a no-NAT policy, specify all of the match criteria and select **No Source Translation** in the source translation column.

Bi-directional NAT Rules

The bi-directional setting in static source NAT rules implicitly creates a destination NAT rule for traffic to the same resources in the reverse direction. In this example, two NAT rules are used to create a source translation for outgoing traffic from IP 10.0.1.10 to public IP 3.3.3.1 and a destination translation for traffic destined for public IP 3.3.3.1 to private IP 10.0.1.10. This pair of rules can be simplified by configuring only the third NAT rule using the bi-directional feature.



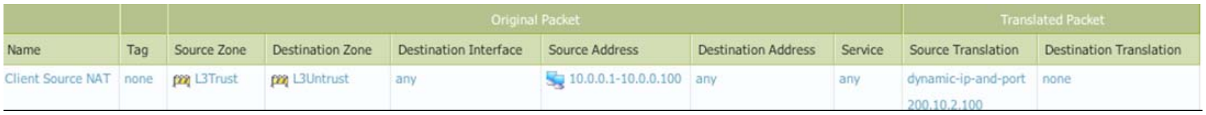
		Original Packet						Translated Packet	
Name	Tag	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
sourcenat	none	L3Trust	L3Untrust	any	10.0.1.10	any	any	static-ip 3.3.3.1 bi-directional: false	none
destnat	none	L3Untrust	L3Trust	any	any	3.3.3.1	any	none	address: 10.0.1.10
bothnat	none	L3Trust	L3Untrust	any	10.0.1.10	any	any	static-ip 3.3.3.1 bi-directional: true	none

Figure 2. Bi-Directional NAT Rules

NAT Policy Examples

The following NAT policy rule translates a range of private source addresses (10.0.0.1 to 10.0.0.100 in the "L3Trust" zone) to a single public IP address (200.10.2.100 in the "L3Untrust" zone) and a unique source port number (dynamic source translation). The rule applies only to traffic received on a Layer 3 interface in the "L3Trust" zone that is destined for an interface in the "L3Untrust" zone. Because the private addresses are hidden, network sessions cannot be initiated from the public network. If the public address is not a firewall interface address (or on the same subnet), the local router requires a static route to direct return traffic to the firewall.

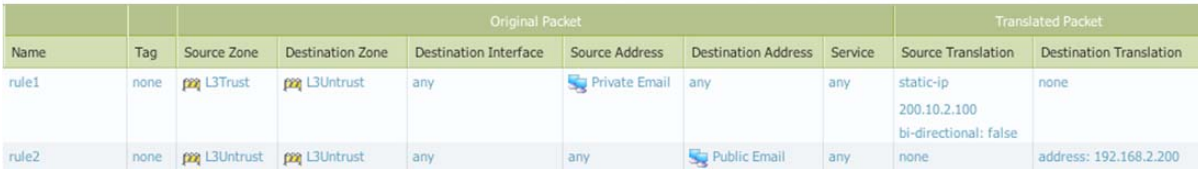
Security policy must be explicitly configured to permit traffic matching this NAT rule. Create a security policy with source/destination zones and source/destination addresses matching the NAT rule.



		Original Packet						Translated Packet	
Name	Tag	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Client Source NAT	none	L3Trust	L3Untrust	any	10.0.0.1-10.0.0.100	any	any	dynamic-ip-and-port 200.10.2.100	none

Figure 3. Dynamic Source Address Translation

In the following example, the first NAT rule translates the private address of an internal mail server to a static public IP address. The rule applies only to outgoing email sent from the "L3Trust" zone to the "L3Untrust" zone. For traffic in the reverse direction (incoming email), the second rule translates the destination address from the server's public address to its private address. Rule2 uses "L3Untrust" for the source and destination zones because NAT policy is based on the pre-NAT address zone. In this case, that pre-NAT address is a public IP address and is therefore in the "L3Untrust" zone.



		Original Packet						Translated Packet	
Name	Tag	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
rule1	none	L3Trust	L3Untrust	any	Private Email	any	any	static-ip 200.10.2.100 bi-directional: false	none
rule2	none	L3Untrust	L3Untrust	any	any	Public Email	any	none	address: 192.168.2.200

Figure 4. Static Source and Destination Address Translation

In both examples, if the public address is not the address of the firewall's interface (or on the same subnet), you must add a static route to the local router to route traffic to the firewall.

NAT64

NAT64 is used to translate source and destination IP headers between IPv6 and IPv4 addresses. It allows IPv6 clients to access IPv4 servers and allows IPv4 clients to access IPv6 servers. There are three main transition mechanisms defined by the IETF: dual-stack, tunneling, and translation. When you have IPv4-only and IPv6-only networks and communication is required, you must use translation.

When using NAT64 policies on Palo Alto Networks firewall, it's required that you have a third-party DNS64 solution in place to decouple the DNS query function from the NAT function.

The following NAT64 features are supported:

- Stateful NAT64, which allows preserving of IPv4 addresses so that one IPv4 address can map to multiple IPv6 addresses. An IPv4 address can also be shared with NAT44. In contrast, stateless NAT64 maps one IPv4 address to one IPv6 address.
- IPv4-initiated communication translation. The static binding for IPv4 maps an IPv4 address/port number to an IPv6 IP address. PAN-OS® also supports port rewrite that allows you to preserve even more IPv4 addresses.
- Allows translation for /32, /40, /48, /56, /64, and /96 subnets.
- Support for multiple prefixes. You can assign one NAT64 prefix per rule.
- Does not require you to reserve a pool of IPv4 address specifically for NAT64. Therefore, it is possible to use a single IP address to do NAT44 and NAT64.
- Supports hairpinning (NAT U-Turn) and it can prevent hairpinning loop attacks.
- Supports the translation of TCP/UDP/ICMP packets as per RFC, but also other protocols without ALG (best effort). For example, a GRE packet could be translated. This translation has the same limitation as NAT44.
- Supports PMTUD (path MTU discovery) and it updates the MSS (Maximum Segment Size) for TCP.
- Allows configuration of the IPv6 MTU setting. The default value is 1280, which is the minimum MTU for IPv6 traffic. This setting is configured in **Device > Setup > Sessions** tab under **Session Settings**.
- Translates length attribute between IPv4 and IPv6.
- Supported on Layer 3 interfaces and subinterfaces, tunnel, and VLAN interfaces.

NAT64 Examples

You can configure two types of translation with the firewall: IPv6-initiated communication, which is similar to source NAT in IPv4, and IPv4-initiated communication to an IPv6 server, which is similar to destination NAT in IPv4.

IPv6-initiated Communication

In this type of translation, the destination IPv6 address in the NAT rule is a prefix following the RFC 6052 format (/32, /40,/48,/56,/64, and /96). The destination IPv6 address netmask in the rule would be used to extract the IPv4 address. The source translation needs to have "Dynamic IP and Port" in order to implement a stateful NAT64. The IPv4 address set as the source is configured the same way as a NAT44 source translation. The destination translation field is not set. However, a destination translation must be done since the address is extracted from the IPv6 address in the packet. It uses prefix defined in the destination IP matching criteria. You should note that in a /96 prefix, it is the last 4 octets, but the location of the IPv4 address would be different if the prefix is not /96.

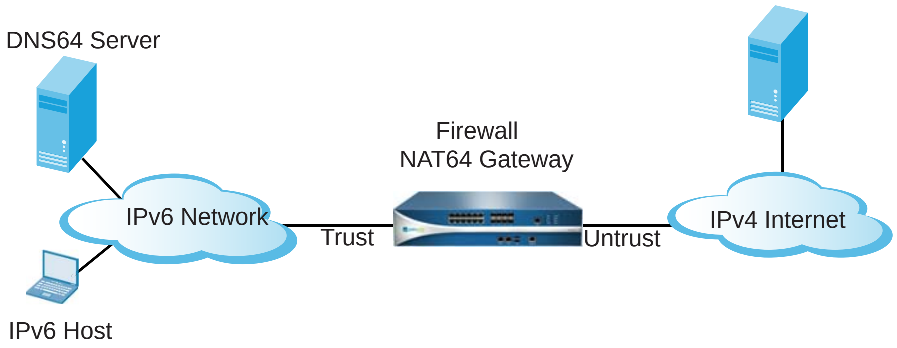


Figure 5. NAT64 IPv6 Client to IPv4 Network

The following table describes the values needed in this NAT64 policy.

Table 137.

Source IP	Destination IP	Source Translation	Destination Translation
Any/IPv6 address	NAT64 IPv6 prefix with RFC6052 compliant netmask	Dynamic IP and port mode (Use IPv4 address)	None (Extracted from the destination IPv6 address)

IPv4-initiated Communication

The IPv4 address is the address that maps to the IPv6 address and you use static IP mode in the source translation. The source would be set in an IPv6 prefix as defined in RFC6052 and is appended to the IPv4 source address. The destination address is the IP address set in the destination translation column. It is possible to rewrite the destination port. This method allows a single IP address to share multiple IPv6 servers through the port through a static mapping.

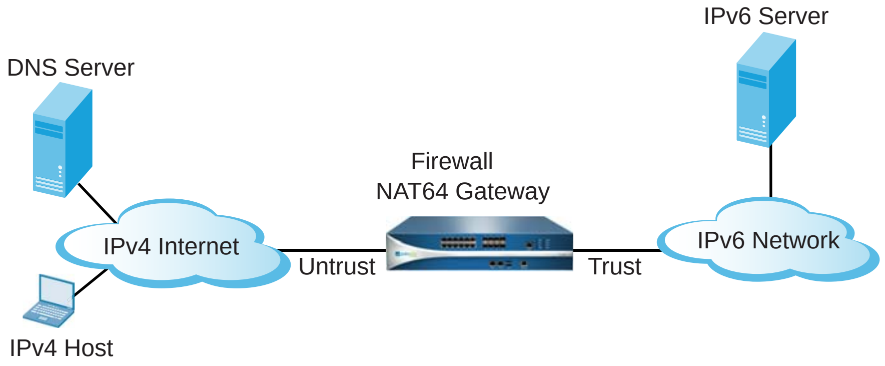


Figure 6. NAT64 IPv4 Internet to IPv6 Customer Network

The following table describes the values needed in this NAT64 policy.

Table 138. IPv4-initiated Values

Source IP	Destination IP	Source Translation	Destination Translation
Any/IPv4 address	IPv4 address	Static IP mode (IPv6 prefix in RFC 6052 format)	Single IPv6 address (actual server IP address) Note: You could specify a server port re-write.

The packet processing engine of the firewall must do a route lookup to find the destination zone prior to looking at the NAT rule. In NAT64, it is important to address the reachability of the NAT64 prefix for the destination zone assignment since the NAT64 prefix should not be routable by the NAT64 gateway. It is very likely that the NAT64 prefix would hit the default route, or be dropped because there is no route. You can setup a tunnel interface with no termination point since this type of interface will act like a loopback port and accept other netmasks besides /128. You apply the NAT64 prefix to the tunnel and apply the appropriate zone in order to ensure that IPv6 traffic with NAT64 prefix is assigned to the proper destination zone. It would also have the advantage to drop the IPv6 traffic with NAT64 prefix if the NAT64 rule is not matched.

IETF Scenarios for IPv4/IPv6 Translation

There are six NAT64 based scenarios defined by the IETF in RFC 6144. The Palo Alto Networks firewall supports all but one of these scenarios, as described in the following table.

Table 139. Summary of IETF Scenario Implementations for Using PAN-OS

Scenario	Source IP	Destination IP	Source Translation	Destination Translation
IPv6 Network to the IPv4 Internet	Any/IPv6 address	NAT64 IPv6 prefix with RFC 6052 compliant netmask.	Dynamic IP and port mode. Use *Public* IPv4 address	None (extracted from destination IPv6 address)
The IPv4 Internet to an IPv6 Network	Any/IPv4 address	Single IPv4 address	Static IP mode. IPv6 Prefix in RFC 6052 format	Single IPv6 address
The IPv6 Internet to an IPv4 Network	Any/IPv6 address	IPV6 globally routable prefix with RFC 6052 compliant netmask.	Dynamic IP and port. Use *Private* IPv4 address	None (extracted from destination IPv6 address)
IPv4 network to IPv6 Internet	Not currently supported			
IPv4 network to IPv6 network	Any/IPv4 address	Single IPv4 address	Static IP mode. IPv6 Prefix in RFC 6052 format	Single IPv6 address
IPv6 network to IPv4 network	Any/IPv6 address	NAT64 IPV6 prefix with RFC 6052 compliant netmask.	Dynamic IP and port. Use Private IPv4 address	None (extracted from destination IPv6 address)

- **Static IP**—For inbound or outbound traffic. You can use static IP to change the source or the destination IP address while leaving the source or destination port unchanged. When used to map a single public IP address to multiple private servers and services, destination ports can stay the same or be directed to different destination ports.

You may need to define static routes on the adjacent router and/or the firewall to ensure that traffic sent to a public IP address is routed to the appropriate private address. If the public address is the same as the firewall interface (or on the same subnet), then a static route is not required on the router for that address. When you specify service (TCP or UDP) ports for NAT, the pre-defined HTTP service (service-http) includes two TCP ports: 80 and 8080. To specify a single port, such as TCP 80, you must define a new service.

The next table summarizes the NAT types. The two dynamic methods map a range of client addresses (M) to a pool (N) of NAT addresses, where M and N are different numbers. N can also be 1. Dynamic IP/Port NAT differs from Dynamic IP NAT in that the TCP and UDP source ports are not preserved in Dynamic IP/Port, whereas they are unchanged with Dynamic IP NAT. There are also differing limits to the size of the translated IP pool, as noted below.

With Static IP NAT, there is a one-to-one mapping between each original address and its translated address. This can be expressed as 1-to-1 for a single mapped IP address, or M-to-M for a pool of many one-to-one, mapped IP addresses.

Table 140. NAT Types

PAN-OS NAT Type	Source Port Stays the Same	Destination Port Can Change	Mapping Type	Size of Translated Address Pool
Dynamic IP/ Port	No	No	Many-to-1 M-to-N	Up to 254 consecutive addresses
Dynamic IP	Yes	No	M-to-N	Up to 32k consecutive addresses
Static IP	Yes	No	1-to-1 M-to-M MIP	Unlimited
	Optional		1-to-Many VIP PAT	

Defining Network Address Translation Policies

▶ ***Policies > NAT***

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.

For information on defining policies on Panorama, see “Defining Policies on Panorama”.

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

- "General Tab"
- "Original Packet Tab"
- "Translated Packet Tab"

General Tab

Use the **General** tab to configure a name and description for the NAT or NPTv6 policy. A tag can also be configured 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.

Table 141. NAT Rule Settings (General Tab)

Field	Description
Name	Enter a name to identify the rule. The name is case-sensitive and can have up to 31 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 255 characters).
Tag	If you want to tag the policy, click **Add** to 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 could 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.
NAT Type	Specify the type of translation the rule is for: • **ipv4** for translation between IPv4 addresses. • **nat64** for translation between IPv6 and IPv4 addresses. • **nptv6** for translation between IPv6 prefixes. You cannot combine IPv4 and IPv6 address ranges in a single NAT rule.

Original Packet Tab

Use the **Original Packet** tab to define the source and destination traffic that will be translated, and the type of destination interface and type of service. Multiple source and destinations zones of the same type can be configured and the rule can be set to apply to specific networks or specific IP addresses.

Table 142. NAT Rule Settings (Original Packet Tab)

Field	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 "Defining Security Zones". Multiple zones can be used 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 type of interface for translation. The destination interface can be used to translate IP addresses differently in the case where the network is connected to two ISPs with different IP address pools.
Service	Specify the services for which the source or destination address is translated. To define new service groups, refer to "Service Groups".
Source Address Destination Address	Specify a combination of source and destination addresses to be translated. 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.

Translated Packet Tab

Use the **Translated Packet** tab to determine, for Source Address Translation, the type of translation to perform on the source, and the address and/or port to which the source will be translated.

Destination Address Translation can also be configured for an internal host that needs to be accessed by a public IP address. In this case, you define a source address (public) and destination address (private) in the **Original Packet** tab for an internal host, and in the **Translated Packet** tab you enable **Destination Address Translation** and enter the **Translated Address**. When the public address is accessed, it will be translated to the internal (destination) address of the internal host.

Table 143. NAT Rule Settings (Translated Packet Tab)

Field	Description
Source Address Translation	Select the Translation Type (dynamic or static address pool), and enter an IP address or address range (address1-address2) that the source address is translated to (**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 will use the same translated source address for all sessions. Dynamic IP and Port source NAT supports approximately 64k concurrent sessions on each IP address in the NAT pool. On some platforms, over-subscription is supported, which will allow a single IP to host more than 64k concurrent sessions. Palo Alto Networks Dynamic IP/port NAT supports more NAT sessions than are supported by the number of available IP addresses and ports. The firewall can use IP address and port combinations up to two times (simultaneously) on the PA-200, PA-500, PA-2000 Series and PA-3000 Series firewalls, four times on the PA-4020 and PA-5020 firewalls, and eight times on the PA-4050, PA-4060, PA-5050, and PA-5060 firewalls when destination IP addresses are unique. • **Dynamic IP**—The next available address in the specified range is used, but the port number is unchanged. Up to 32k 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 (Fall back Dynamic IP Translation)**—Use this option to create a fall back pool that will perform IP and port translation and will be 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, which is for interfaces that receive an IP address dynamically. When creating a fall back pool, make sure addresses do not overlap with addresses in the primary pool. • **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. – NPTv6 must use **Static IP** translation for Source Address Translation. For NPTv6, the prefixes configured for **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. • **None**—Translation is not performed.

Table 143. NAT Rule Settings (Translated Packet Tab) (Continued)

Field	Description
Bi-directional	(Optional) Enable bi-directional 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 Bi-directional translation, it is very important to make sure you have security policies in place to control the traffic in both directions. Without such policies, the Bi-directional feature will allow packets to be automatically translated in both directions, which you might not want.
Destination Address Translation—Translated Address	Enter an IP address or range of IP addresses and a translated port number (1 to 65535) that the destination address and port number are translated to. If the **Translated Port** field is blank, the destination port is not changed. Destination translation is typically used to allow an internal server, such as an email server, to be accessed from the public network. For NPTv6, the prefixes configured for 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. Note that Translated Port is not supported for NPTv6 because NPTv6 is strictly prefix translation. The Port and Host address section is simply forwarded unchanged.

Policy-Based Forwarding Policies

▶ *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. With policy-based forwarding (PBF), 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.

For configuration guidelines and information on other policy types, refer to "Policies and Security Profiles".

For information on defining policies on Panorama, see "Defining Policies on Panorama".

The following tables describe the policy-based forwarding settings:

- "General Tab"
- "Source Tab"
- "Destination/Application/Service Tab"

- “Forwarding Tab”

General Tab

Use 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 31 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 255 characters).
Tag	If you need to tag the policy, click **Add** to 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.

Source Tab

Use 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 list. To define new zones, refer to “Defining Security 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. **Note:** 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 list, or click the **Address**, **Address Group**, or **Regions** link at the bottom of the drop-down list, and specify the settings.

Field	Description
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 clients, 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 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. **Note:** *If you are using a RADIUS server and not the User-ID Agent, the list of users is not displayed, and you must enter user information manually.*

Destination/Application/Service Tab

Use 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, address groups, or regions (default is any). By default, the rule applies to **Any** IP address. Select from the drop-down list, or click the **Address**, **Address Group**, or **Regions** link at the bottom of the drop-down list, 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 “Defining Application Groups”. **Note:** *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. For details, see https://paloaltonetworks.com/documentation/70/pan-os/pan-os/policy/pbf.html.* If you are using application groups, filters, or container in the PBF rule, you can view details on these objects 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 members directly from the policy without having to go to the Object tabs.

Forwarding Tab

Use 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 list. • **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.
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 IP address for the packet.
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) that specifies the action when the IP address is unreachable.
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 (say, 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 list. To define new schedules, refer to “SSL Decryption Settings in a Decryption Profile”.

Decryption Policies

▶ *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.

Each decryption policy specifies the categories of URLs to decrypt or not decrypt. SSL decryption can be used to apply App-ID and the Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-blocking profiles to decrypted SSL traffic before it is re-encrypted as traffic exits the device. You can apply decryption profiles to any decryption policy to block and control various aspects of traffic. For more information, refer to "Decryption Profiles". With decryption enabled, end-to-end security between clients and servers is maintained, and the firewall acts as a trusted third party during the connection. No decrypted traffic leaves the device.

Decryption policies can be as general or specific as needed. The policy rules are compared against the traffic in sequence, so more specific rules must precede the more general ones. To move a rule to the top of the policies so that the rule takes precedence, select the rule and click Move Up. A policy that excludes traffic from decryption (with the **No Decrypt** action enabled) should always take precedence in order to be effective.

SSL forward proxy decryption requires the configuration of a trusted certificate that will be presented to the user if the server to which the user is connecting possesses a certificate signed by a CA trusted by the firewall. To configure this certificate, create a certificate on the **Device > Certificate Management > Certificates** page and then click the name of the certificate and check the **Forward Trust Certificate** check box. Refer to "Managing Device Certificates".

For configuration guidelines and information on other policy types, refer to "Policies and Security Profiles".

For information on defining policies on Panorama, see "Defining Policies on Panorama".

Certain applications will not function if they are decrypted by the firewall. To prevent this from occurring, PAN-OS will not decrypt the SSL traffic for these applications and the decryption rule settings will not apply.
For a list of these applications, refer to support article located at https://live.paloaltonetworks.com/docs/DOC-1423.

The following tables describe the decryption policy settings:

- "General Tab"
- "Source Tab"
- "Destination Tab"
- "Service/URL Category Tab"
- "Options Tab"

General Tab

Use the **General** tab to configure a name and description for the decryption 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 31 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 255 characters).

Field	Description
Tag	If you need to tag the policy, click **Add** to 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.

Source Tab

Use 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 "Defining Security 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 list, or click the **Address**, **Address Group**, or **Regions** link at the bottom of the drop-down list, and specify the settings. Select the **Negate** check box 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 clients, 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 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. **Note:** *If you are using a RADIUS server and not the User-ID Agent, the list of users is not displayed, and you must enter user information manually.*

Destination Tab

Use 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 “Defining Security 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 list, or click the **Address**, **Address Group**, or **Regions** link at the bottom of the drop-down list, and specify the settings. Select the **Negate** check box to choose any address except the configured ones.

Service/URL Category Tab

Use 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 list: • **any**—The selected applications are allowed or denied on any protocol or port. • **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**. Refer to “Services” and “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 list. You can add multiple categories. Refer to “Dynamic Block Lists” for information on defining custom categories.

Options Tab

Use 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.

Field	Description
Type	Select the type of traffic to decrypt from the drop-down list: • **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	Select an existing decryption profile, or create a new decryption profile. Refer to “Decryption Profiles”.

Defining Application Override Policies

▶ *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”).

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:

1. Define the custom application. Refer to “Defining Applications”. It is not required to specify signatures for the application if the application is used only for application override rules.

2. 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.

For configuration guidelines and information on other policy types, refer to “Policies and Security Profiles”.

For information on defining policies on Panorama, see “Defining Policies on Panorama”.

Use the following tables to configure an application override rule.

- “General Tab”
- “Source Tab”
- “Destination Tab”
- “Protocol/Application Tab”

General Tab

Use 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 31 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 255 characters).
Tag	If you need to tag the policy, click **Add** to 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.

Source Tab

Use 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	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 “Defining Security 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 list, or click the **Address**, **Address Group**, or **Regions** link at the bottom of the drop-down list, and specify the settings. Select the **Negate** check box to choose any address except the configured ones.

Destination Tab

Use 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 "Defining Security 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 list, or click the **Address**, **Address Group**, or **Regions** link at the bottom of the drop-down list, and specify the settings. Select the **Negate** check box to choose any address except the configured ones.

Protocol/Application Tab

Use 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 for which the application can be overridden.
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 "Defining Applications").

Defining Captive Portal Policies

Policies > Captive Portal

Use the following table to set up and customize a captive portal to direct user authentication by way of an authentication profile, an authentication sequence, or a certificate profile. Captive portal is used in conjunction with the User-ID Agent to extend user identification functions beyond the Active Directory domain. Users are directed to the portal and authenticated, thereby creating a user-to-IP address mapping.

Before defining captive portal policies, enable captive portal and configure captive portal settings on the **User Identification** page, as described in "Configuring the Firewall for User Identification".

For configuration guidelines and information on other policy types, refer to "Policies and Security Profiles".

The following tables describe the captive portal policy settings:

- "General Tab"

- "Source Tab"
- "Destination Tab"
- "Service/URL Category Tab"
- "Action Tab"

General Tab

Use the General tab to configure a name and description for the captive portal 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 31 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 255 characters).
Tag	If you need to tag the policy, click **Add** to 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.

Source Tab

Use the **Source** tab to define the source zone or source address that defines the incoming source traffic to which the captive portal policy will be applied

Field	Description
Source	Specify the following information: • Choose a source zone if the policy needs to be applied to traffic coming from all interfaces in a given zone. Click **Add** to specify multiple interfaces or zones. • Specify the **Source Address** setting to apply the captive portal policy for traffic coming from specific source addresses. Select the **Negate** check box to choose any address except the configured ones. Click **Add** to specify multiple interfaces or zones.

Destination Tab

Use 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	Specify the following information: • Choose a destination zone if the policy needs to be applied to traffic to all interfaces in a given zone. Click **Add** to specify multiple interfaces or zones. • Specify the **Destination Address** setting to apply the captive portal policy for traffic to specific destination addresses. Select the **Negate** check box to choose any address except the configured ones. Click **Add** to specify multiple interfaces or zones.

Service/URL Category Tab

Use the **Service/URL Category** tab to have the policy action occur based on a specific TCP and/or UDP port numbers. A URL Category can also be used as an attribute for the policy.

Field	Description
Service	Select services to limit to specific TCP and/or UDP port numbers. Choose one of the following from the drop-down list: • **any**—The selected services are allowed or denied on any protocol or port. • **default**—The selected services are allowed or denied only on the 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. Refer to “Services” and “Service Groups”.
URL Category	Select URL categories for the captive portal rule. • Choose **any** to apply the actions specified on the **Service/Action** tab regardless of the URL category. • To specify a category, click **Add** and select a specific category (including a custom category) from the drop-down list. You can add multiple categories. Refer to “Dynamic Block Lists” for information on defining custom categories.

Action Tab

Use the **Action** tab to determine if the user will see a web-form, a browser-challenge dialogue, or if no captive portal challenge should occur.

Field	Description
Action Setting	Choose an action to take: • **web-form**—Present a captive portal page for the user to explicitly enter authentication credentials. • **no-captive-portal**—Allow traffic to pass without presenting a captive portal page for authentication. • **browser-challenge**—Open an NT LAN Manager (NTLM) authentication request to the user's web browser. The web browser will respond using the user’s current login credentials.

Defining DoS Policies

▶ *Policies > DoS Protection*

DoS protection policies allow you to 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.

A DoS policy can include a DoS profile that specifies the thresholds (sessions or packets per second) that indicate an attack. In policy, you can then select a protective action when a match is triggered. See “DoS Profiles”.

For information on defining policies on Panorama, see “Defining Policies on Panorama”.

Use this page to add, edit, or delete DoS protection policy rules. To add a policy rule, click **Add** and then complete the following fields:

General Tab

Use the **General** tab to configure a name and description for the DoS 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 31 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 255 characters).
Tag	If you need to tag the policy, click **Add** to 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.

Source Tab

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

Field	Description
Source	Specify the following information: • Choose **Interface** from the **Type** drop-down list to apply the DoS policy to traffic coming from an interface or a group of interfaces. Choose **Zone** if the DoS policy needs to be applied to traffic coming from all interfaces in a given zone. Click **Add** to specify multiple interfaces or zones. • Specify the **Source Address** setting to apply the DoS policy for traffic coming from specific source addresses. Select the **Negate** check box to choose any address except the configured ones. Click **Add** to specify multiple addresses. • Specify the **Source User** setting to apply the DoS policy for traffic from specific users. The following source user types are supported: – **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 their system. When the Pre-logon option is configured on the Portal for GlobalProtect clients, 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 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. **Note:** *If you are using a RADIUS server and not the User-ID Agent, the list of users is not displayed, and you must enter user information manually.*

Destination Tab

Use 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	Specify the following information: • Choose **Interface** from the **Type** drop-down list to apply the DoS policy to traffic coming from an interface or a group of interfaces. Choose **Zone** if the DoS policy needs to be applied to traffic coming from all interfaces in a given zone. Click **Add** to specify multiple interfaces or zones. • Specify the **Destination Address** setting to apply the DoS policy for traffic to specific destination addresses. Select the **Negate** check box to choose any address except the configured ones. Click **Add** to specify multiple addresses.

Options/Protection Tab

Use the **Options/Protection** tab to configure additional options for the DoS policy, such as the type of service (http or https), the action to take, and whether or not to trigger a log forward for matched traffic. You can also define a schedule for when the policy will be active and select an aggregate or classified DoS profile that defines more attributes for DoS protection.

Field	Description
Service	Select from the drop-down list to apply the DoS policy to only the configured services.
Action	Choose the action from the drop-down list: • **Deny**—Drop all traffic. • **Allow**—Permit all traffic. • **Protect**—Enforce protections supplied in the thresholds that are configured as part of the DoS profile applied to this rule.
Schedule	Select a pre-configured schedule from the drop-down list to apply the DoS rule to a specific date/time.
Log Forwarding	If you want to trigger forwarding of threat log entries to an external service—such as a syslog server or Panorama—select a log forwarding profile from the drop-down or click **Profile** to create a new one. Note that only traffic that matches an action in the rule will be logged and forwarded.
Aggregate	Select a DoS protection profile from the drop-down list to determine the rate at which you want to take action in response to DoS threats. The aggregate setting applies to the total of all traffic from the specified source to specified destination.

Field	Description
Classified	Select the check box and specify the following: • **Profile**—Select the profile from the drop-down list. • **Address**—Select whether to apply the rule to the source, destination, or source and destination IP addresses. If a classified profile is specified, the profile limitations are applied to a source IP address, destination IP address, or source and destination IP address pair. For example, you could specify a classified profile with a session limit of 100 and specify an **Address** setting of "source" in the rule. The result would be a limit of 100 sessions at any given time for that particular source IP address.

Security Profiles

Security profiles provide threat protection in security policies. Each security policy can include one or more security profile.

The following profile types are available:

- Antivirus profiles to protect against worms, viruses, and trojans and to block spyware downloads. See "Antivirus Profiles".
- 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 "Anti-Spyware Profiles".
- Vulnerability protection profiles to stop attempts to exploit system flaws or gain unauthorized access to systems. See "Vulnerability Protection Profiles".
- URL filtering profiles to restrict users access to specific websites and/or website categories, such as shopping or gambling. See "URL Filtering Profiles".
- File blocking profiles to block selected file types, and in the specified session flow direction (inbound/outbound/both). See "File Blocking Profiles".
- WildFire Analysis profiles to specify for file analysis to be performed locally on the WildFire appliance or in the WildFire cloud. See "WildFire Analysis Profiles".
- Data filtering profiles that help prevent sensitive information such as credit card or social security numbers from leaving a protected network. See "Data Filtering Profiles".

In additional to individual profiles, you can combine profiles that are often applied together, and create security profile groups in **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, or custom vulnerability objects.

Action	Description	Antivirus Profile	Anti-Spyware profile	Vulnerability Protection Profile	Custom Object—Spyware and Vulnerability
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.	✓	✓	✓	✗
Allow	Permits the application traffic.	✓	✓	✓	✓
Alert	Generates an alert for each application traffic flow. The alert is saved in the threat log.	✓	✓	✓	✓
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	✓	✓	✓	✓
Reset Both	For TCP, resets the connection on both client and server ends. For UDP, the connection is dropped	✓	✓	✓	✓
Block IP	This action blocks traffic from either a source or a source-destination pair; Configurable for a specified period of time.	✗	✓	✓	✓

You cannot delete a profile that is used in a security policy. You must first remove the profile from the security policy, then delete it.

Antivirus Profiles

▶ *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 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.

For a list of all security profile type s and the actions that can be taken on matched traffic, see “Security Profiles”.

The following tables describe the policy-based forwarding settings:

- “Antivirus Profile Dialog”
- “Antivirus Tab”
- “Exceptions Tab”

Antivirus Profile Dialog

Use this dialog to define a name and description for the profile.

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	Select this check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.

Antivirus Tab

Use the Antivirus tab to define the type of traffic that will be inspected, such as ftp, and http, and then specify the action to take. You can define different actions for standard antivirus signatures (Action column) and signatures generated by the WildFire system (WildFire 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 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.

Use the **Applications Exception** table to define applications that will not be inspected. For example, you may want to allow http, but not inspect traffic from a specific application that operates over http.

Field	Description
Packet Capture	Select the check box 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 list. You can also take specific action based on signatures created by WildFire.
Applications Exceptions and Actions	Identify applications that will be exceptions to the antivirus rule. 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. 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. The application is added to the table, and you can assign an action. 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”

Exceptions Tab

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

Field	Description
Threat ID	Add specific threats that should be ignored. Exceptions that are already specified are listed. You can add additional threats by entering the threat ID and clicking **Add**. Threat IDs are presented as part of the threat log information. Refer to “Viewing the Logs”.

Anti-Spyware Profiles

▶ *Objects > Security Profiles > Anti-Spyware*

You can attach an Anti-Spyware profile to a security policy for detecting "phone home" connections that are initiated from spyware installed on systems on your network.

You can choose between two predefined Anti-Spyware profiles in security policy. Each of these profiles 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 Palo Alto Networks 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 block 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 **Rules** settings 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.

The **Exceptions** settings 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 content updates so that you are protected against new threats and have new signatures for any false-positives.

The **DNS Signatures** settings provides an additional method of identifying infected hosts on a network. These signatures detect specific DNS lookups for host names that have been associated with malware. The DNS signatures can be configured to allow, alert, or (default) block when these queries are observed, just as with regular antivirus signatures. Additionally, hosts that perform DNS queries for malware domains will appear in the botnet report. DNS signatures are downloaded as part of the antivirus updates.

The **Anti-Spyware** 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. For more information, refer to "Locking Transactions".

The following tables describe the Anti-Spyware profile settings:

Table 144. Anti-Spyware Profile Settings

Field	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).

Table 144. Anti-Spyware Profile Settings (Continued)

Field	Description
Shared	Select this check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Rules Tab	
Rule Name	Specify the rule name.
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.
Severity	Choose a severity level (**critical**, **high**, **medium**, **low**, or **informational**).
Action	Choose an action for each threat. For a list of actions, see “Actions in Security Profiles”.
Packet Capture	Select the check box 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. Extended-capture will provides much more context to the threat when analyzing the threat logs. To view the packet capture, navigate to **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, navigate to **Device > Setup > Content-ID** and then edit the **Content-ID Settings** section. Packet captures will only occur if the action is allow or alert. If the block action is set, the session is ended immediately.
Exceptions Tab	
Exceptions	Select the **Enable** check box 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. Use the IP Address Exemptions column 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 will only be taken over the rule's action if the signature is triggered by a session having either the source or destination IP matching an IP 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.
DNS Signature Tab	

Table 144. Anti-Spyware Profile Settings (Continued)

Field	Description
Action on DNS queries	Choose an action to be taken when DNS lookups are made to known malware sites (allow, block, sinkhole, or default (alert)). 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 (i.e. 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 will 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 will identify 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. After selecting the sinkhole action, specify an IPv4 and/or IPv6 address that will be used as the sinkhole (the default is the loopback IP, which will resolve domains to the local host). When a sinkhole IP address is configured, the infected clients can be identified by filtering the traffic logs or by building a custom report that checks for sessions to the specified IP address. It is important to choose an IP address that results in a session having to be routed through the firewall in order for the firewall to see the session, for example an unused IP in another internal zone. The following is the sequence of events that will occur when the sinkhole feature is enabled: 1. Malicious software on an infected client computer sends a DNS query to resolve a malicious host on the Internet. 2. 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. 3. The DNS query matches a DNS entry in the DNS signatures database, so the sinkhole action will be performed on the query. 4. 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. 5. 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.
Packet Capture	Select the check box if you want to capture identified packets.

Table 144. Anti-Spyware Profile Settings (Continued)

Field	Description
Enable Passive DNS Monitoring	This an opt-in feature that enables the firewall to act as a passive DNS sensor and send select DNS information to Palo Alto Networks for analysis in order to improve threat intelligence and threat prevention capabilities. The data collected includes non-recursive (i.e. originating from the local recursive resolver, not individual clients) DNS query and response packet payloads. This information is used by the Palo Alto Networks threat research team to gain insights into malware propagation and evasion techniques that abuse the DNS system. Information gathered through this data collection is used to improve accuracy and malware detection abilities within PAN-DB URL filtering, DNS-based command-and-control signatures, and WildFire. The recommended setting for this feature is to enable it. *When the firewall is configured with custom service routes, the Passive DNS feature will use the WildFire service route to send the DNS information to Palo Alto Networks.* The option is disabled by default.
Threat ID	Manually enter DNS signature exceptions (range 4000000-4999999).

Vulnerability Protection Profiles

▶ ***Objects > Security Profiles > Vulnerability Protection***

A security policy 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 **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 “Defining Security Policies”.

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. For more information, refer to “Locking Transactions”.

The following tables describe the Vulnerability Protection profile settings:

Table 145. Vulnerability Protection Profile Settings

Field	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	Select this check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
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.
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, navigate to Objects > Security Profiles > Vulnerability Protection and click **Add** or select an existing profile. Click the **Exceptions** tab and then click **Show all signatures**. A list of all signatures will displayed and you will see an **Action** column.
Host	Specify whether to limit the signatures for the rule to those that are client side, server side, or either (**any**).
Packet Capture	Select the check box 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. Extended-capture will provides much more context to the threat when analyzing the threat logs. To view the packet capture, navigate to **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, navigate to **Device > Setup > Content-ID** and then edit the **Content-ID Settings** section. Packet captures will only occur if the action is allow or alert. If the block action is set, the session is ended immediately.
Category	Select a vulnerability category if you want to limit the signatures to those that match that category.

Table 145. Vulnerability Protection Profile Settings (Continued)

Field	Description
CVE List	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”.
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 MS*yy-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”.
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.
Exceptions Tab	
Threats	Select the **Enable** check box 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. Choose an action from the drop-down list box, or choose from the **Action** drop-down at the top of the list to apply the same action to all threats. If the **Show All** check box is selected, all signatures are listed. If the **Show All** check box is not selected, only the signatures that are exceptions are listed. Select the **Packet Capture** check box if you want to capture identified packets. 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 the pencil icon ✏ next to the threat name on the **Vulnerability** tab (with the **Custom** option selected). You 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. The* ***CVE*** *column shows identifiers for common vulnerabilities and exposures (CVE). These unique, common identifiers are for publicly known information security vulnerabilities.* Use the IP Address Exemptions column 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 will only be taken over the rule's action if the signature is triggered by a session having either the source or destination IP matching an IP 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.

URL Filtering Profiles

▶ *Objects > Security Profiles > URL Filtering*

A security policy can include specification of a URL filtering profile that blocks access to specific web sites and web site categories, enforces safe search, or generates an alert when the specified web sites are accessed (a URL filtering license is required). You can also define a “block list” of web sites that are always blocked (or generate alerts) and an “allow list” of web sites that are always allowed.

To apply URL filtering profiles to security policies, refer to “Defining Security Policies”. To create custom URL categories with your own lists of URLs, refer to “Custom URL Categories”.

The following tables describe the URL filtering profile settings:

Table 146. URL Filtering Profile Settings

Field	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 check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Categories	
(Configurable for BrightCloud only) Action on License Expiration	Select the action to take if the URL filtering license expires: • **Block**—Blocks access to all web sites. • **Allow**—Allows access to all web sites. **Note:** *If you are using the BrightCloud database and you set this option to Block upon license expiration, all URLs will be blocked, not just the URL categories that are set to block. If you set to Allow, all URLs will be allowed.* *If the license expires for PAN-DB, URL filtering is not enforced:* • *URL categories that are currently in cache will be used to either block or allow content based on your configuration. Using cached results is a security risk because the categorization information might be stale.* • *URLs that are not in the cache will be categorized as not-resolved and will be allowed.* *Always renew your license in time to ensure network security.*

Table 146. URL Filtering Profile Settings (Continued)

Field	Description
Block List	Enter the IP addresses or URL path names of the web sites that you want to block or generate alerts on. Enter each URL one per line. **IMPORTANT:** You must omit the “http and https” portion of the URLs when adding web sites to the list. Entries in the block list are an exact match and are case-insensitive. For example, "www.paloaltonetworks.com” is different from "paloaltonetworks.com". If you want to block the entire domain, you should include both "*.paloaltonetworks.com" and "paloaltonetworks.com". Examples: • www.paloaltonetworks.com • 198.133.219.25/en/US Block and allow lists support wildcard patterns. The following characters are considered separators: *.* */* *?* *&* *=* *;* *+* Every substring that is separated by the characters listed above is considered a token. A token can be any number of ASCII characters that does not contain any separator character or *. For example, the following patterns are valid: **.yahoo.com* *(Tokens are: "*", "yahoo" and "com")* *www.*.com* *(Tokens are: "www", "*" and "com")* *www.yahoo.com/search=** *(Tokens are: "www", "yahoo", "com", "search", "*")* The following patterns are invalid because the character “*” is not the only character in the token. *ww*.yahoo.com* *www.y*.com*
Action	Select the action to take when a web site in the block list is accessed. • **alert**—Allow the user to access the web site, but add an alert to the URL log. • **block**—Block access to the web site. • **continue**—Allow the user to access the blocked page by clicking **Continue** on the block page. • **override**—Allow the user to access the blocked page after entering a password. The password and other override settings are specified in the URL Admin Override area of the **Settings** page (refer to the Management Settings table in “Defining Management Settings”).

Table 146. URL Filtering Profile Settings (Continued)

Field	Description
Allow List	Enter the IP addresses or URL path names of the web sites that you want to allow or generate alerts on. Enter each IP address or URL one per line. **IMPORTANT:** You must omit the “http and https” portion of the URLs when adding web sites to the list. Entries in the allow list are an exact match and are case-insensitive. For example, "www.paloaltonetworks.com” is different from "paloaltonetworks.com". If you want to allow the entire domain, you should include both "*.paloaltonetworks.com" and "paloaltonetworks.com". Examples: • www.paloaltonetworks.com • 198.133.219.25/en/US Block and allow lists support wildcard patterns. The following characters are considered separators: *.* */* *?* *&* *=* *;* *+* Every substring that is separated by the characters listed above is considered a token. A token can be any number of ASCII characters that does not contain any separator character or *. For example, the following patterns are valid: **.yahoo.com (Tokens are: "*", "yahoo" and "com")* *www.*.com (Tokens are: "www", "*" and "com")* *www.yahoo.com/search=* (Tokens are: "www", "yahoo", "com", "search", "*")* The following patterns are invalid because the character “*” is not the only character in the token. *ww*.yahoo.com* *www.y*.com* This list takes precedence over the selected web site categories.
Category/Action	For each category, select the action to take when a web site of that category is accessed. • **alert**—Allow the user to access the web site, but add an alert to the URL log. • **allow**—Allow the user to access the web site. • **block**—Block access to the web site. • **continue**—Allow the user to access the blocked page by clicking **Continue** on the block page. • **override**—Allow the user to access the blocked page after entering a password. The password and other override settings are specified in the URL Admin Override area of the **Settings** page (refer to the Management Settings table in “Defining Management Settings”). **Note:** *The Continue and Override pages will not be displayed properly on client machines that are configured to use a proxy server.*

Table 146. URL Filtering Profile Settings (Continued)

Field	Description
Check URL Category	Click to access the web site where you can enter a URL or IP address to view categorization information.
Dynamic URL Filtering Default: Disabled (Configurable for BrightCloud only) *With PAN-DB, this option is enabled by default and is not configurable.*	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 window, the response is displays as “Not resolved URL.”
Log container page only Default: Enabled	Select the check box to log only the URLs that match the content type that is specified.
Enable Safe Search Enforcement Default: Disabled To use this feature, a URL filtering license is not required.	Select this check box to enforce strict safe search filtering. When enabled, this option will prevent users who are searching the Internet using one of the following search providers—Bing, Google, Yahoo, Yandex, or YouTube—from viewing the search results unless the strictest safe search option is set in their browsers for these search engines. If a user performs a search using one of these search engines and their browser or search engine account setting for safe search is not set to strict, the search results will be blocked (depending on the action set in the profile) and the user will be prompted to set their safe search setting to strict. **Note:** *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 enforce safe search, the profile must be added to a security policy. And, to enable safe search for encrypted sites (HTTPS), the profile must be attached to a decryption policy. The ability of the firewall to detect the safe search setting within these three providers will be updated using the Applications and Threats signature update. If a provider changes the safe search setting method that Palo Alto Networks uses to detect the safe search settings, an update will be made to the signature update to ensure that the setting is detected properly. Also, the evaluation to determine whether a site is judged to be safe or unsafe is performed by each search provider, not Palo Alto Networks. 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. Refer to the PAN-OS 7.0 Administrator’s Guide for more information.

Table 146. URL Filtering Profile Settings (Continued)

Field	Description
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.

File Blocking Profiles

▶ *Objects > Security Profiles > File Blocking*

A security policy can include specification of a file blocking profile that blocks selected file types from being uploaded and/or downloaded, or generates an alert when the specified file types are detected. If the **forward** action is selected, supported file types will be sent to WildFire where they will be analyzed for malicious behavior. Table 148 lists the supported file formats at the time of this publication. However, because new file type support can be added in a content update, for the most up-to-date list, click **Add** in the **File Types** field of the File Blocking Profile dialog.

To apply file blocking profiles to security policies, refer to "Defining Security Policies".

The following tables describe the file blocking profile settings:

Table 147. File Blocking Profile Settings

Field	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).

Table 147. File Blocking Profile Settings (Continued)

Field	Description
Shared	Select this check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
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**—Select the file types for which you want to block or generate alerts. • **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. – **block**—The file is blocked. – **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*** *or* ***continue-and-forward*** *(used for WildFire forwarding), you can only choose the application* ***web-browsing****. If you choose any other application, traffic that matches the security policy will not flow through the firewall due to the fact that the users will not be prompted with a continue page.* – **forward**—The file is automatically sent to WildFire. – **continue-and-forward**—A continue page is presented, and the file is sent to WildFire (combines the **continue** and **forward** actions). This action only works with web-based traffic. This is due to the fact that a user must click continue before the file will be forward and the continue response page option is only available with http/https.

Table 148. Supported File Formats for File Blocking

Field	Description
apk	Android application package file
avi	Video file based on Microsoft AVI (RIFF) file format
avi-divx	AVI video file encoded with the DivX codec
avi-xvid	AVI video file encoded with the XviD codec
bat	MS DOS Batch file
bmp-upload	Bitmap image file (upload only)
cab	Microsoft Windows Cabinet archive file
cdr	Corel Draw file
class	Java bytecode file
cmd	Microsoft command file
dll	Microsoft Windows Dynamic Link Library
doc	Microsoft Office Document
docx	Microsoft Office 2007 Document
dpx	Digital Picture Exchange file
dsn	Database Source Name file
dwf	Autodesk Design Web Format file
dwg	Autodesk AutoCAD file
edif	Electronic Design Interchange Format file
email-link	By forwarding the email-link file type, the firewall extracts HTTP/HTTPS links contained in SMTP and POP3 email messages and forward the links to the WildFire cloud for analysis (this feature is not supported on the WF-500 WildFire appliance). Note that the firewall only extracts links and associated session information (sender, recipient, and subject) from the email messages that traverse the firewall; it does not receive, store, forward, or view the email message. After receiving an email link from a firewall, WildFire visits the links to determine if the corresponding web page hosts any exploits. If it determines that the page itself is benign, no log entry will be sent to the firewall. If the link is malicious, a WildFire detailed analysis report is generated in the firewall’s WildFire Submissions log and the URL is added to PAN-DB.
encrypted-doc	Encrypted Microsoft Office Document
encrypted-docx	Encrypted Microsoft Office 2007 Document
encrypted-office2007	Encrypted Microsoft Office 2007 File
encrypted-pdf	Encrypted Adobe PDF Document
encrypted-ppt	Encrypted Microsoft Office PowerPoint
encrypted-pptx	Encrypted Microsoft Office 2007 PowerPoint
encrypted-rar	Encrypted rar file
encrypted-xls	Encrypted Microsoft Office Excel

Table 148. Supported File Formats for File Blocking (Continued)

Field	Description
encrypted-xlsx	Encrypted Microsoft Office 2007 Excel
encrypted-zip	Encrypted zip file
exe	Microsoft Windows Executable
flash	Includes the Adobe Shockwave Flash SWF and SWC file types. The SWF file delivers vector graphics, text, video, and sound over the Internet and the content is viewed using the Adobe Flash player. The SWC file is a compressed package of SWF components.
flv	Adobe Flash Video file
gds	Graphics Data System file
gif-upload	GIF image file (upload only)
gzip	Files compressed with gzip utility
hta	HTML Application file
iso	Disc Image file based on ISO-9660 standard
iwork-keynote	Apple iWork Keynote documents
iwork-numbers	Apple iWork Numbers documents
iwork-pages	Apple iWork Pages documents
jar	Java ARchive
jpeg-upload	JPG/JPEG image file (upload only)
lnk	Microsoft Windows file shortcut
lzh	File compressed with lha/lzh utility/algorithm
mdb	Microsoft Access Database file
mdi	Microsoft Document Imaging file
mkv	Matroska Video file
mov	Apple Quicktime Movie file
mp3	MP3 audio file
mp4	MP4 audio file
mpeg	Movie file using MPEG-1 or MPEG-2 compression
msi	Microsoft Windows Installer package file
msoffice	Microsoft Office File (doc, docx, ppt, pptx, pub, pst, rtf, xls, xlsx). If you want the firewall to block/forward MS Office files, it is recommended that you select this “msoffice” group to ensure all supported MS Office file types will be identified instead of selecting each file type individually.

Table 148. Supported File Formats for File Blocking (Continued)

Field	Description
Multi-Level-Encoding	File that has been encoded five or more times. Multiple levels of file encoding can be an indicator of suspicious behavior. Files might be compressed multiple times with the intention concealing the original file type and evading detection for malicious content. By default, the firewall decodes and identifies files that have been encoded up to four times; however, you can use this file type to block files that are not decoded by the firewall due to being encoded five or more times.
ocx	Microsoft ActiveX file
pdf	Adobe Portable Document file
PE	Microsoft Windows Portable Executable (exe, dll, com, scr, ocx, cpl, sys, drv, tlb)
pgp	Security key or digital signature encrypted with PGP software
pif	Windows Program Information File containing executable instructions
pl	Perl Script file
png-upload	PNG image file (upload only)
ppt	Microsoft Office PowerPoint Presentation
pptx	Microsoft Office 2007 PowerPoint Presentation
psd	Adobe Photoshop Document
rar	Compressed file created with winrar
reg	Windows Registry file
rm	RealNetworks Real Media file
rtf	Windows Rich Text Format document file
sh	Unix Shell Script file
stp	Standard for the Exchange of Product model data 3D graphic file
tar	Unix tar archive file
tdb	Tanner Database (www.tannereda.com)
tif	Windows Tagged Image file
torrent	BitTorrent file
wmf	Windows Metafile to store vector images
wmv	Windows Media Video file
wri	Windows Write document file
wsf	Windows Script file
xls	Microsoft Office Excel
xlsx	Microsoft Office 2007 Excel
zcompressed	Compressed Z file in Unix, decompressed with uncompress
zip	Winzip/pkzip file

WildFire Analysis Profiles

▶ *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).

Table 149. WildFire Analysis Profile Settings

Field	Description
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. 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	Select this check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
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. • 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.

Data Filtering Profiles

▶ *Objects > Security Profiles > Data Filtering*

A security policy can include specification of a data filtering profile to help identify sensitive information such as credit card or social security numbers and prevent the sensitive information from leaving the area protected by the firewall.

To apply data filtering profiles to security policies, refer to “Defining Security Policies”.

The following tables describe the data filtering profile settings:

Table 150. Data Filtering Profile Settings

Field	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	Select this check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Data Capture	Select the check box 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 "Defining Management Settings".*

To add a data pattern, click **Add** and specify the following information.

Table 151. Data Pattern Settings

Field	Description
Data Pattern	Choose an existing data pattern from the Data Pattern drop-down list, or configure a new pattern by choosing **Data Pattern** from the list and specifying the information described in "Defining 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: • 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.

Table 151. Data Pattern Settings (Continued)

Field	Description
Alert Threshold	Specify the value that will trigger an alert. For example, if you have a threshold of 100 with a SSN weight of 5, the rule will need to detect at least 20 SSN patterns before the rule will be triggered (20 instances x 5 weight = 100).
Block Threshold	Specify the value that will trigger a block. For example, if you have a threshold of 100 with a SSN weight of 5, the rule will need to detect at least 20 SSN patterns before the rule will be triggered (20 instances x 5 weight = 100).

DoS Profiles

▶ ***Objects > Security Profiles > DoS Protection***

DoS protection profiles are designed for high precision targeting and augment zone protection profiles. The DoS profile specifies the types of actions and the matching criteria to detect a DoS attack. These profiles are attached to DoS protection policies to allow you to control traffic between interfaces, zones, addresses, and countries based on aggregate sessions or unique source and/or destination IP addresses. To apply DoS profiles to DoS policies, refer to “Defining DoS Policies”.

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, 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

The following tables describe the DoS protection profile settings:

Table 152. DoS Protection Profile Settings

Field	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.
Shared	Select this check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Description	Enter a description of the profile (up to 255 characters).
Type	Specify one of the following profile types: • **aggregate**—Apply the DoS thresholds configured in the profile to all packets that match the rule criteria on which this profile is applied. For example, an aggregate rule with a SYN flood threshold of 10000 packets per second (pps) counts all packets that hit that particular DoS rule. • **classified**—Apply the DoS thresholds configured in the profile to all packets satisfying the classification criterion (source IP, destination IP or source-and-destination IP).

Table 152. DoS Protection Profile Settings (Continued)

Field	Description
Flood Protection Tab	
Syn Flood subtab UDP Flood subtab ICMP Flood subtab ICMPv6 subtab Other IP subtab	Select the check box to enable the type of flood protection indicated on the tab, and specify the following settings: • **Action**—(SYN Flood only) Choose from the following options: – **Random Early Drop**—Drop packets randomly before the overall DoS limit is reached. – **SYN cookies**—Use SYN cookies to generate acknowledgments so that it is not necessary to drop connections in the presence of a SYN flood attack. • **Alarm Rate**—Specify the threshold rate (pps) at which a DoS alarm is generated. (Range is 0-2000000 pps; default is 10000 pps). • **Activate Rate**—Specify the threshold rate (pps) at which a DoS response is activated. The DoS response is configured in the **Action** field of the DoS policy where this profile is referenced. When the **Activate Rate** threshold is reached, **Random Early Drop** occurs. (Range is 0-2000000 pps; default is 10000 pps). • **Max Rate**—Specify the threshold rate of incoming packets per second the firewall allows. When the threshold is exceeded, new packets that arrive are dropped and the Action in the DoS policy is triggered. (Range is 2-2000000 pps; default is 40000 pps.) • **Block Duration**—Specify the length of time (seconds) during which the offending packets will be denied. Packets arriving during the block duration do not count toward triggered alerts. (Range is 1-21600 seconds; default is 300 seconds.) **Note:** *When defining packets per second (pps) thresholds limits for zone and DoS protection profiles, the threshold is based on the packets per second that do not match a previously established session.*
Resources Protection Tab	
Sessions	Select the check box to enable resources protection.
Max Concurrent Limit	Specify the maximum number of concurrent sessions. If the DoS profile type is aggregate, this limit applies to the entire traffic hitting the DoS rule on which the DoS profile is applied. If the DoS profile type is classified, this limit applies to the entire traffic on a classified basis (source IP, destination IP or source-and-destination IP) hitting the DoS rule on which the DoS profile is applied.

Other Policy Objects

Policy objects are the elements that enable you to construct, schedule, and search for policies. The following object types are supported:

- Addresses and address groups to determine the scope of the policy. See “Defining Address Groups”.
- Applications and application groups that allow you to specify how software applications are treated in policies. See “Applications”.
- Application filters that allow you to simplify searches. See “Application Filters”.

- Services and service groups to limit the port numbers. See “Services”.
- Tags to sort and filter objects. See “Tags”.
- Data patterns to define categories of sensitive information for data filtering policies. See “Data Patterns”.
- Custom URL categories that contain your own lists of URLs to include as a group in URL filtering profiles. See “Custom URL Categories”.
- Spyware and vulnerability threats to allow for detailed threat responses. See “Security Profile Groups”.
- Log forwarding to specify log settings. See “Log Forwarding”.
- Schedules to specify when policies are active. See “SSL Decryption Settings in a Decryption Profile”.

To move or clone objects, see “Moving or Cloning a Policy or Object”.

Defining Address Objects

▶ *Objects > Addresses*

An address object can include an IPv4 or IPv6 address (single IP, range, subnet) or a FQDN. It allows you to reuse the same object as a source or destination address across all the policy rulebases without having to add it manually each time. It is configured using the web interface or the CLI and a commit operation is required to make the object a part of the configuration.

To define an address object, click **Add** and fill in the following fields:

Table 153. New Address Settings

Field	Description
Name	Enter a name that describes the addresses to be defined (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 check box if you want the address object to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the address object will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the address object will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the address in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Description	Enter a description for the object (up to 255 characters).

Table 153. New Address Settings (Continued)

Field	Description
Type	Specify an IPv4 or IPv6 address or address range, or FQDN. **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. Example: “192.168.80.150/32” indicates one address, and “192.168.80.0/24” indicates all addresses from 192.168.80.0 through 192.168.80.255. Example: “2001:db8:123:1::1” or “2001:db8:123:1::/64” **IP Range:** To specify an address range, select **IP Range**, and enter a range of addresses. The format is: *ip_address–ip_address* where each address can be IPv4 or IPv6. Example: “2001:db8:123:1::1 - 2001:db8:123:1::22”
Type (continued)	**FQDN:** To specify an address using the FQDN, select **FQDN** and enter the domain name. The FQDN initially resolves at commit time. Entries are subsequently refreshed when the firewall performs a check every 30 minutes; all changes in the IP address for the entries are picked up at the refresh cycle The FQDN is resolved by the system DNS server or a DNS proxy object, if a proxy is configured. For information about DNS proxy, refer to “Configuring DNS Proxy”.
Tags	Select or enter the tags that you wish to apply to this address object. You can define a tag here or use the Objects > Tags tab to create new tags. For information on tags, see “Tags”.

Defining Address Groups

▶ *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.

Unlike a static address group where you specify the network address of a host, the members of a dynamic address group are populated using a match criteria that you define. The match criteria uses logical *and* or *or* operators; each host that you want to add to the dynamic address group must bear the tag or attribute that is defined in the match criteria. Tags can be defined directly on the firewall or on Panorama or they can be dynamically defined using the XML API and registered with the firewall. When an IP address and the corresponding tag (one or more) is registered, each dynamic group evaluates the tags and updates the list of members in its group.

In order to register new IP address and tags or changes to current IP addresses and tags, you must use scripts that call the XML API on the firewall. If you have a virtual environment with VMware, instead of using scripts calling the XML API, you can use the VM Information Sources feature (**Device > VM Information Sources** tab) to configure the firewall to monitor the ESX(i) host or the vCenter Server and retrieve information (network address and corresponding tags) on new servers/guests deployed on these virtual machines.

In order 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. This can be done either using external scripts that use the XML API on the firewall or for a VMware-based environment it can be configured on the **Device > VM Information Sources** tab 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:

Table 154. Address Group

Field	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 check box if you want the address group to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the address group will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the address group will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the address group in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Description	Enter a description for the object (up to 255 characters).
Type	Select **Static** or **Dynamic**. 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. **Note:** *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 “Tags”.

Defining Regions

▶ *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:

Table 155. New Region Settings

Field	Description
Name	Enter a name that describes the region (up to 31 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.
Geo Location	To specify latitude and longitude, select the check box and values (*xxx.xxxxxx* format). This information is used in the traffic and threat maps for App-Scope. Refer to "Using App Scope".
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*

Applications

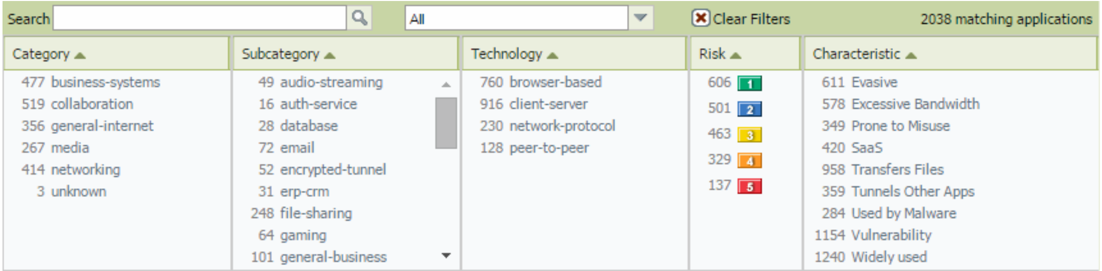
▶ *Objects > Applications*

What are you looking for?	See
Understand the application settings and attributes displayed on the **Applications** page.	▶ *"Applications Overview"*
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.



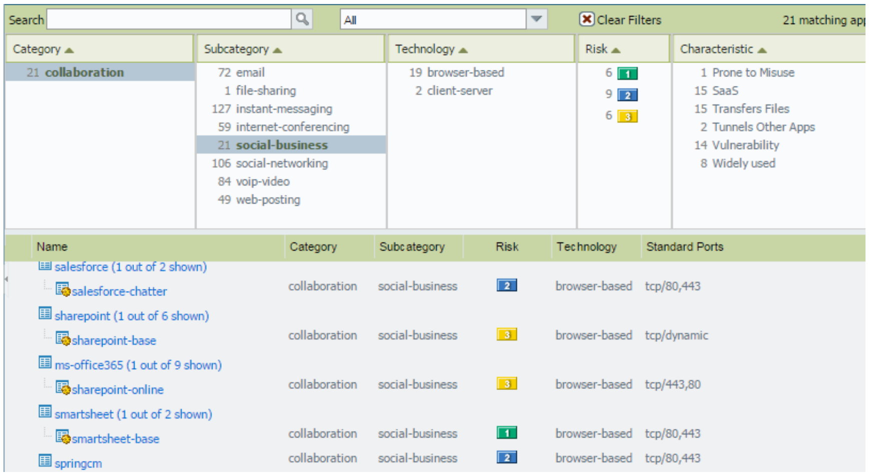
2038 matching applications

Category ▲	Subcategory ▲	Technology ▲	Risk ▲	Characteristic ▲
477 business-systems	49 audio-streaming	760 browser-based	606 1	611 Evasive
519 collaboration	16 auth-service	916 client-server	501 2	578 Excessive Bandwidth
356 general-internet	28 database	230 network-protocol	463 3	349 Prone to Misuse
267 media	72 email	128 peer-to-peer	329 4	420 SaaS
414 networking	52 encrypted-tunnel		137 5	958 Transfers Files
3 unknown	31 erp-crm			359 Tunnels Other Apps
	248 file-sharing			284 Used by Malware
	64 gaming			1154 Vulnerability
	101 general-business			1240 Widely used

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

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

- To apply application filters, 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** and the list will only show applications in this category.



Category	Subcategory	Technology	Risk	Characteristic
21 **collaboration**	72 email	19 browser-based	6 1	1 Prone to Misuse
	1 file-sharing	2 client-server	9 2	15 SaaS
	127 instant-messaging		6 3	15 Transfers Files
	59 internet-conferencing			2 Tunnels Other Apps
	21 **social-business**			14 Vulnerability
	106 social-networking			8 Widely used
	84 voip-video			
	49 web-posting			

Name	Category	Subcategory	Risk	Technology	Standard Ports
salesforce (1 out of 2 shown)					
salesforce-chatter	collaboration	social-business	2	browser-based	tcp/80,443
sharepoint (1 out of 6 shown)					
sharepoint-base	collaboration	social-business	3	browser-based	tcp/dynamic
ms-office365 (1 out of 9 shown)					
sharepoint-online	collaboration	social-business	3	browser-based	tcp/443,80
smartsheet (1 out of 2 shown)					
smartsheet-base	collaboration	social-business	1	browser-based	tcp/80,443
springcm	collaboration	social-business	2	browser-based	tcp/80,443

- To filter on additional columns, select an entry in the other columns. The filtering is successive: first Category filters are applied, 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 has not been explicitly applied. Each time you apply a filter, the list of applications in the lower part of the page automatically updates. View any saved filters in **Objects > Application Filters**.

- To search for a specific application, enter the application name or description in the **Search** field, and press **Enter**. 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.

- 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.

- Select a disabled application and **Enable** the application so that it can be enforced according to your configured security policies.

- To import an application, click **Import**. Browse to select the file, and select the target virtual system from the **Destination** drop-down list.

- To export an application, select the check box for the application and click **Export**. Follow the prompts to save the file.
- **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; 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.
- To view additional details about the application or to customize risk and timeout values, as described in the following table, click an application name. If the icon to the left of the application name has a yellow pencil on it, the application is a custom application. Note that the settings available vary by application.

The following tables describe the application settings:

Table 156. Application Details

Item	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 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 new App-IDs, or App-IDs that have been 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 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.
Characteristic	
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.

Table 156. Application Details (Continued)

Item	Description
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).
Transfers Files	Has the capability to transfer a file from one system to another over a network.
Tunnels Other Apps	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.
Vulnerability	Has publicly reported vulnerabilities.
Widely used	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.
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	
browser-based	An application that relies on a web browser to function.
client-server	An application that uses a client-server model where one or more clients communicate with a server in the network.

Table 156. Application Details (Continued)

Item	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.
Risk	
	Assigned risk of the application. To customize this setting, click the **Customize** link, enter a value (1-5), and click **OK**.
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 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.

Table 156. Application Details (Continued)

Item	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 “Working with Botnet Reports”.

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.

Defining Applications

▶ *Objects > Applications*

Use the **Applications** page to **Add** a new application for the firewall to evaluate when applying policies.

Table 157. New Application Settings

Field	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 check box if you want the application to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the application will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the application will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the application in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
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 “Using the Application Command Center”).
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 “Using the Application Command Center”).
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.
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 “Characteristic”.
Advanced Tab	

Table 157. New Application Settings (Continued)

Field	Description
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 0-255).
ICMP6 Type	To specify an Internet Control Message Protocol version 6 (ICMPv6) type, select **ICMP6 Type** and enter the type number (range 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 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 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 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 sec. 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 sec. If this value is configured at the application level, it overrides the global TCP Time Wait setting.
Scanning	Select check boxes for the scanning types that you want to allow, based on security profiles (file types, data patterns, and viruses).

Table 157. New Application Settings (Continued)

Field	Description
Signature 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. • **Scope**—Select whether to apply this signature only to the current transaction or to the full user session. • **Ordered Condition Match**—Select if the order in which signature conditions are defined is important. Specify conditions to 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**. • Select an operator from **Pattern Match** and **Equal To**. When choosing a **Pattern Match** operator, specify the following: – **Context**—Select from the available contexts. – **Pattern**—Specify a regular expression. See Table 163 for pattern rules for regular expressions. – **Qualifier and Value**—Optionally, add qualifier/value pairs. • When choosing an **Equal To** operator, specify the following, – **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. • To move a condition within a group, select the condition and click the **Move Up** or **Move Down** arrow. To move a group, select the group and click the **Move Up** or **Move Down** arrow. 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.

To import an application, click **Import**. Browse to select the file, and select the target virtual system from the **Destination** drop-down list.

To export the application, select the check box for the application and click **Export**. Follow the prompts to save the file.

Defining Application Groups

▶ *Objects > Application Groups*

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

Table 158. New Application Group

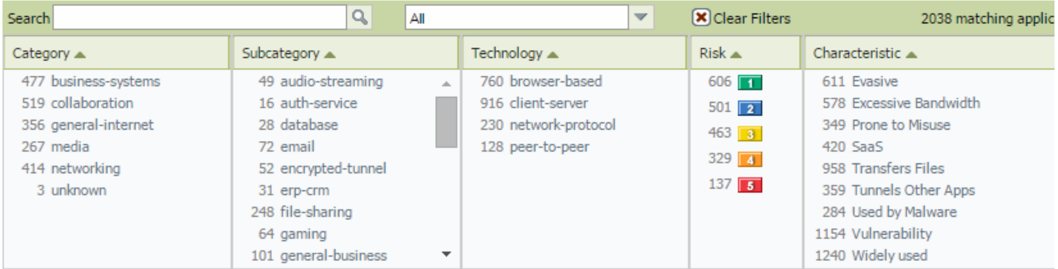
Field	Description
Name	Enter a name that describes the application group (up to 31 characters). This name appears in the application list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this check box if you want the application group to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the application group will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the application group will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the application group in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Applications	Click **Add** and select applications, application filters, and/or other application groups to be included in this group.

Application Filters

▶ *Objects > Application Filters*

You can define application filters to simplify repeated searches. To define application filters to simplify repeated searches, click **Add** and enter a name for the 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 Networking category, click **networking**.

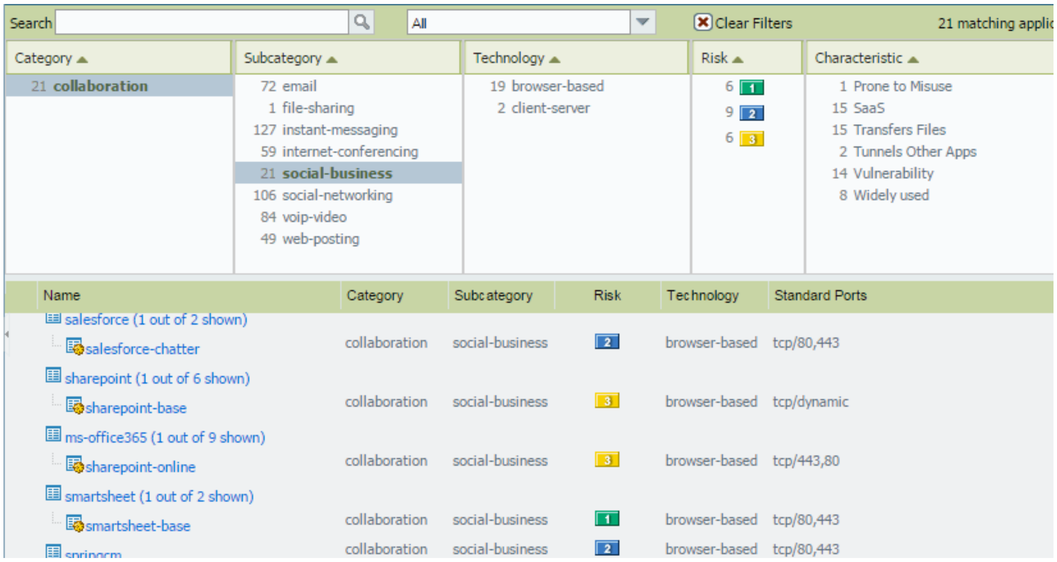


Category	Subcategory	Technology	Risk	Characteristic
477 business-systems	49 audio-streaming	760 browser-based	606 1	611 Evasive
519 collaboration	16 auth-service	916 client-server	501 2	578 Excessive Bandwidth
356 general-internet	28 database	230 network-protocol	463 3	349 Prone to Misuse
267 media	72 email	128 peer-to-peer	329 4	420 SaaS
414 networking	52 encrypted-tunnel		137 5	958 Transfers Files
3 unknown	31 erp-crm			359 Tunnels Other Apps
	248 file-sharing			284 Used by Malware
	64 gaming			1154 Vulnerability
	101 general-business			1240 Widely used

To filter on additional columns, select an entry in the columns to display check boxes. The filtering is successive: first category filters are applied, then subcategory filters, then technology filters, then risk, filters, and finally characteristic filters.

For example, the next figure shows the result of choosing a category, subcategory, and risk filter. In applying the first two filters, the Technology column is automatically restricted to the technologies that are consistent with the selected category and subcategory, even though a technology filter has not been explicitly applied.

As you select options, the list of applications in the lower part of the page is automatically updated, as shown in the figure.



Category	Subcategory	Technology	Risk	Characteristic
21 collaboration	72 email	19 browser-based	6 1	1 Prone to Misuse
	1 file-sharing	2 client-server	9 2	15 SaaS
	127 instant-messaging		6 3	15 Transfers Files
	59 internet-conferencing			2 Tunnels Other Apps
	21 social-business			14 Vulnerability
	106 social-networking			8 Widely used
	84 voip-video			
	49 web-posting			

Name	Category	Subcategory	Risk	Technology	Standard Ports
salesforce (1 out of 2 shown)					
salesforce-chatter	collaboration	social-business	2	browser-based	tcp/80,443
sharepoint (1 out of 6 shown)					
sharepoint-base	collaboration	social-business	3	browser-based	tcp/dynamic
ms-office365 (1 out of 9 shown)					
sharepoint-online	collaboration	social-business	3	browser-based	tcp/443,80
smartsheet (1 out of 2 shown)					
smartsheet-base	collaboration	social-business	1	browser-based	tcp/80,443
springcm	collaboration	social-business	2	browser-based	tcp/80,443

Services

▶ *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 “Service Groups”).

The following table describes the service settings:

Table 159. Service Settings

Field	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 255 characters).
Shared	Select this check box if you want the service object to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the service object will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the service object will be available only to the **Device Group** selected in the **Objects** tab.

Table 159. Service Settings (Continued)

Field	Description
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the service object in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
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.

Service Groups

▶ *Objects > Services 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 "Services".

The following table describes the service group settings:

Table 160. Service Group Settings

Field	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 check box if you want the service group to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the service group will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the service group will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the service group in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Service	Click **Add** to add services to the group. Select from the drop-down list, or click the **Service** button at the bottom of the drop-down list, and specify the settings. Refer to "Services" for a description of the settings.

Tags

▶ *Objects > Tags*

Tags allow you to group objects using keywords or phrases. Tags can be applied to address objects, address groups (static and dynamic), zones, services, service groups, and to policy rules. You can use a tags to sort or filter objects, and to visually distinguish objects because they can have color. When a color is applied to a tag, the **Policy** tab displays the object with a background color.

What do you want to know?	See
How do I create tags?	▶ *"Create Tags"*
What is the tag browser?	▶ *"Use the Tag Browser"*
How do I search for rules that are tagged? How do I group rules using tags? How do I view tags used in policy? How can I apply tags to policy?	▶ *"Manage Tags"*
Do you want more?	**See** Policy

Create Tags

▶ *Objects > Tags*

Use this tab to create a tag, assign a color, 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 to it.

*On the firewall, the **Objects >Tags** tab displays the tags that you define locally on the firewall or push from Panorama to the firewall; on Panorama, it 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, or tags that are defined using the XML 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.

- Add a tag: To add a new tag, click **Add** and then fill in the following fields:

Table 161. Tag Settings

Field	Description
Name	Enter a unique tag name (up to 127 characters). The name is not case-sensitive.
Shared	Select this check box if you want the tag to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the tag will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the tag will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the tag in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Color	Select a color from the color palette in the drop-down list. The default value is None.
Comments	Add a label or description to remind you what the tag is used for.

  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: To edit, rename, or assign a color to a tag, click the tag name that displays as a link and modify the settings.

- Delete a tag: To delete a tag, click **Delete** and select the tag in the window.

- Move or Clone a tag: The option to move to clone a tag allows you copy a tag or move the tag to a different Device Group or Virtual System on devices enabled for multiple virtual systems.

  Click **Clone** or **Move** and select the tag in the window. Select the **Destination** location—Device Group or Virtual System—for the tag. Clear the check box for **Error out on first detected error in validation** if you want the validation process to discover all the errors for the object before displaying the errors. By default, the check box is enabled and the validation process stops when the first error is detected and only displays the error.

- Override or Revert a tag (on Panorama only): The Override option is available if you have not selected the Disable override option when creating the tag. It allows you to override the color assigned to the tag that was inherited from a shared or ancestor device group. The **Location** field displays the current device group. You can also select the Disable override to disable further overrides.

  To undo the changes on a tag, click Revert. When you revert a tag, the **Location** field displays the device group or virtual system from where the tag was inherited.

Use the Tag Browser

▶ ***Policies > Rulebase (Security, NAT, QoS...)***

The tag browser presents a summary of all the tags used within a rulebase (policy set). It allows you to see a list of all the tags and the order in which they are listed in the rulebase.

You can sort, browse, search, and filter for a specific tag, or view only the first tag applied to each rule in the rulebase.

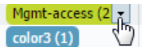
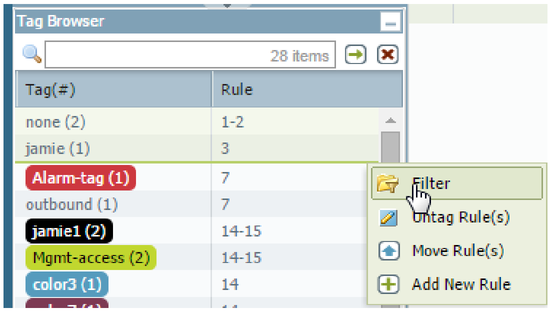
The following table describes the options in the tag browser:

Table 162. Use the Tag Browser

Field	Description
Tag (#)	Displays the label and the rule number or range of numbers in which the tag is used contiguously. Hover over the label to see the location where the rule was defined. The location can be inherited from the **Shared** location, a device group, or a virtual system.
Rule	Lists the rule number or range of numbers associated with the tags.
Filter by first tag in rule	Displays only the first tag applied to each rule in the rulebase, when selected. This view is particularly useful if you want to narrow the list and view related rules that might be spread around the rulebase. For example, if the first tag in each rule denotes its function—administration, web-access, datacenter access, proxy—you can narrow the result and scan the rules based on function.
Rule Order	Sorts the tags in the order of appearance within the selected rulebase. When displayed in order of appearance, tags used in contiguous rules are grouped together. The rule number with which the tag is associated is displayed along with the tag name.
Alphabetical	Sorts the tags in alphabetical order within the selected rulebase. The display lists the tag name, color (if a color is assigned), and the number of times it is used within the rulebase. The label **None** represents rules without any tags; it does not display rule numbers for untagged rules. When you select **None**, the right pane is filtered to display rules that have no tags assigned to them.
Clear	Clears the filter on the currently selected tags in the search bar.
Search bar	Allows you to search for a tag, enter the term and click the green arrow icon to apply the filter. It also displays the total number of tags in the rulebase and the number of selected tags.
For other actions, see “Manage Tags”.	

Manage Tags

The following table lists the actions that you can perform using the tab browser.

Manage Tags	
Tag a rule.	1. Select a rule on the right pane. 2. Do one of the following: – Select a tag in the tag browser and, from the drop-down, select **Apply the Tag to the Selection(s)**.  – Drag and drop tags from the tag browser on to the tag column of the rule. When you drop the tags, a confirmation dialog displays.
	1. Select one or more tags in the tag browser. The tags are filtered using an OR operator. 2. The right pane updates to display the rules that have any of the selected tags. 3. To view the currently selected tags, hover over the **Clear** label in the tag browser.
View the currently selected tags.	To view the currently selected tags, hover over the Clear label in the tag browser.
View rules that match the selected tags. You can filter rules based on tags with an AND or an OR operator.	• OR filter: To view rules that have specific tags, select one or more tags in the tag browser. The right pane will display only the rules that include the currently selected tags. • AND filter: To view rules that have all the selected tags, hover over the number in the **Rule** column of the tag browser and select **Filter** in the drop-down.  Tag Browser 28 items Tag(#) Rule none (2) 1-2 jamie (1) 3 Alarm-tag (1) 7 outbound (1) 7 jamie1 (2) 14-15 Mgmt-access (2) 14-15 color3 (1) 14 Filter Untag Rule(s) Move Rule(s) Add New Rule Repeat to add more tags. Click the → in the search bar on the right pane. The results are displayed using an AND operator.
Untag a rule.	Hover over the rule number in the **Rule** column of the tag browser and select **Untag Rule(s)** in the drop-down. Confirm that you want to remove the selected tag from the rule.

Manage Tags	
Reorder a rule using tags.	Select one or more tags and hover over the rule number in the **Rule** column of the tag browser and select **Move Rule(s)** in the drop-down. Select a 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.	Select one or more tags, hover over the rule number in the **Rule** column of the tag browser, and select **Add New Rule** in the drop-down. The numerical order of the new rule varies by whether you selected a rule on the right pane. If no rule was selected on the right pane, the new rule will be added after the rule to which the selected tag(s) belongs. Otherwise, the new rule is added after the selected rule.
Search for a tag.	In the tag browser, enter the first few letters of the tag name you want to search for and click → . The tags that match your input will display.

Data Patterns

Data pattern support allows you to specify categories of sensitive information that you may want to subject to filtering using data filtering security policies. For instructions on configuring data patterns, refer to “Defining Data Patterns”.

When adding a new pattern (regular expression), the following general requirements apply:

- The pattern must have string of at least 7 bytes to match. It can contain more than 7 bytes, but not fewer.
- The string match may or may not be case-sensitive, depending on which decoder is being used. When case-sensitivity is required, you would need to define patterns for all of the possible strings in order to match all variations of a term. For example, if you wanted to match any documents designated as confidential, you would need to create a pattern for “confidential”, “Confidential”, and “CONFIDENTIAL”.

The regular expression syntax in PAN-OS is similar to traditional regular expression engines, but every engine is unique. The following table describes the syntax supported in PAN-OS.

Table 163. Pattern Rules

Syntax	Description
.	Match any single character.
?	Match the preceding character or expression 0 or 1 time. The general expression MUST be inside a pair of parentheses. Example: (abc)?
*	Match the preceding character or expression 0 or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)*

Table 163. Pattern Rules

Syntax	Description
+	Match the preceding character or regular expression one or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)+
|	Equivalent to “or”. Example: ((bif) | (scr) | (exe)) matches “bif”, “scr” or “exe”. Note that the alternative substrings must be in parentheses.
-	Used to create range expressions. Example: [c-z] matches any character between c and z, inclusive.
[ ]	Match any. Example: [abz]: matches any of the characters a, b, or z.
^	Match any except. Example: [^abz] matches any character except a, b, or z.
{ }	Min/Max number of bytes. Example: {10-20} matches any string that is between 10 and 20 bytes. This must be directly in front of a fixed string, and only supports “-”.
\	To perform a literal match on any one of the special characters above, it MUST be escaped by preceding them with a ‘\’ (backslash).
&amp	& is a special character, so to look for the “&” in a string you must use “&amp” instead.

Data Patterns 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”

Dynamic Block Lists

▶ *Objects > Dynamic Block Lists*

Use the **Dynamic Block Lists** page to create an address object based on an imported list of IP addresses. You must create this list as a text file and save it to a web server that the firewall can access and import; the firewall uses the management port to retrieve this list.

You can configure the firewall to automatically update the list on the device hourly, daily, weekly, or monthly. After creating a dynamic block list object, you can then use the address object in the source and destination fields for security policies.

A maximum of ten dynamic block lists are supported on all platforms. Each list can contain up to 5,000 IP addresses (IPv4 and/or IPv6) that can include IP ranges and/or IP subnets. The list must contain one IP address, range, or subnet per line. Some examples follow:

Single IP address:

IPv4: 192.168.80.150/32

IPv6: 2001:db8:123:1::1 or 2001:db8:123:1::/64

IP Range:

To specify an address range, select **IP Range**, and enter a range of addresses. The format is:

ip_address–ip_address

where each address can be IPv4 or IPv6.

IPv4: “192.168.80.0/24” indicates all addresses from 192.168.80.0 through 192.168.80.255

IPv6: 2001:db8:123:1::1 - 2001:db8:123:1::22

The following table describes the dynamic block list settings:

Table 164 Dynamic Block Lists

Field	Description
Name	Enter a name to identify the dynamic block list (up to 32 characters). This name will appear when selecting the source or destination in a policy.
Shared	Select this check box if you want the dynamic block list to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the dynamic block list will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the dynamic block list will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the dynamic block list in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Description	Enter a description for the dynamic block list (up to 255 characters).
Source	Enter an HTTP or HTTPS URL path that contains the text file. For example, http://1.1.1.1/myfile.txt.

Table 164 Dynamic Block Lists

Field	Description
Repeat	Specify the frequency in which the list should be imported. You can choose hourly, daily, weekly, or monthly. At the specified interval, the list will be imported into the configuration. A full commit is not needed for this type of update to occur.
Test Source URL (firewall only)	Test that the source URL or server path is available. This button is only available in the firewall web interface, not in Panorama.

Custom Spyware and Vulnerability Signatures

This section describes the options available to create custom Spyware and Vulnerability signatures that can be used when creating custom vulnerability profiles.

▶ *Objects > Custom Objects > Data Patterns*

▶ *Objects > Custom Objects > Spyware*

▶ *Objects > Custom Objects > Vulnerability*

▶ *Objects > Custom Objects > URL Category*

Defining Data Patterns

▶ *Objects > Custom Objects > Data Patterns*

Use the **Data Patterns** page to define the categories of sensitive information that you may want to subject to filtering using data filtering security policies. For information on defining data filtering profiles, refer to "Data Filtering Profiles".

The following table describes the data pattern settings:

Table 165. Data Pattern Settings

Field	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 check box if you want the data pattern to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the data pattern will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the data pattern will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the data pattern in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Weight	Enter weights for pre-specified pattern types. The weight is a number between 1 and 255. Alert and Block thresholds specified in the Data Filtering Profile are a function of this weight. • **CC#**—Specify a weight for the credit card field (range 0-255). • **SSN#**—Specify a weight for the social security number field, where the field includes dashes, such as 123-45-6789 (range 0-255, 255 is highest weight). • **SSN# (without dash)**—Specify a weight for the social security number field, where the entry is made without dashes, such as 123456789 (range 0-255, 255 is highest weight).

Table 165. Data Pattern Settings (Continued)

Field	Description
Custom Patterns	The pre-defined patterns include credit card number and social security number (with and without dashes). Click **Add** to add a new pattern. Specify a name for the pattern, enter the regular expression that defines the pattern, and enter a weight to assign to the pattern. Add additional patterns as needed.

Defining Spyware and Vulnerability Signatures

▶ *Objects > Custom Objects > Spyware*

▶ *Objects > Custom Objects > 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.

Table 166. Custom Signatures - Vulnerability and Spyware

Field	Description
Configuration Tab	
Threat ID	Enter a numeric identifier for the configuration. For spyware signatures, the range is 15000-18000; for vulnerability signatures the range is 41000-45000.
Name	Specify the threat name.
Shared	Select this check box if you want the custom signature to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the custom signature will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the custom signature will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the signature in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Comment	Enter an optional comment.
Severity	Assign a level that indicates the seriousness of the threat.

Table 166. Custom Signatures - Vulnerability and Spyware (Continued)

Field	Description
Default Action	Assign the default action to take if the threat conditions are met. For a list of actions, see “Actions in Security Profiles”.
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.

Table 166. Custom Signatures - Vulnerability and Spyware (Continued)

Field	Description
Signatures Tab	
Standard Signature	Select the **Standard** radio button and then click **Add** to 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 list. 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 Table 163 for pattern rules for regular expressions. – **Qualifier and Value**—Optionally, add qualifier/value pairs. – **Negate**—Select the Negate check box 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. **Note:** *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 now 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.

Table 166. Custom Signatures - Vulnerability and Spyware (Continued)

Field	Description
	• 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 the **Combination** radio button. In the area above the subtabs, specify the following information: On the **Combination Signatures** subtab, specify conditions to 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 the **Move Up** or **Move Down** arrow. To move a group, select the group and click the **Move Up** or **Move Down** arrow. You cannot move conditions from one group to another. On the **Time Attribute** subtab, 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 the **Move Up** or **Move Down** arrow. To move a group, select the group and click the **Move Up** or **Move Down** arrow. You cannot move conditions from one group to another.

Custom URL Categories

▶ *Objects > Custom Objects > URL Category*

The custom URL categories feature allows you to create your own lists of URLs that can be selected in any URL filtering profile. Each custom category can be controlled independently and will have an action associated with it in each URL filtering profile (allow, block, continue, override, alert, or none). The *none* action only applies to custom URL categories. The purpose of selecting *none* is to ensure that if multiple URL profiles exist, the custom category will not have any impact on other profiles. For example, if you have two URL profiles and the custom URL category is set to block in one of the profiles, the other profile should have the action set to *none* if you do not want it to apply.

URL entries can be added individually, or you can import a list of URLs. To do so, create a text file that contains the URLs to include, with one URL per line. Each URL can be in the format “www.example.com,” and can contain * as a wildcard, such as “*.example.com.” For additional information on wildcards, refer to the description of the Block List field in the “URL Filtering Profile Settings” table.

URL entries added to custom categories are case insensitive. Also, to delete a custom category after it has been added to a URL profile and an action has been set, the action must be set to None before the custom category can deleted.

For instructions on setting up URL filtering profiles, refer to "URL Filtering Profiles".

The following table describes the custom URL settings:

Table 167. Custom URL Categories

Field	Description
Name	Enter a name to identify the custom URL category (up to 31 characters). This name appears in the category list when defining URL filtering policies. 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).
Shared	Select this check box if you want the URL category to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the URL category will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the URL category will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the URL category in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Sites	In the Sites area, click **Add** to enter a URL or click **Import** and browse to select the text file that contains the list of URLs.

Security Profile Groups

▶ *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 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 new security profiles, refer to "Defining Security Policies".

The following table describes the security profile settings:

Table 168. Security Profile Group Settings

Field	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	Select this check box if you want the profile group to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile group will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile group will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile group in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
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 "Data Filtering Profiles".

Log Forwarding

▶ *Objects > Log Forwarding*

Each security policy can specify a log forwarding profile that determines whether traffic and threat log entries are logged remotely with Panorama, and/or sent as SNMP traps, syslog messages, or email notifications. By default, only local logging is performed.

Traffic logs record information about each traffic flow, and threat logs record the threats or problems with the network traffic, such as virus or spyware detection. Note that the Antivirus, Anti-Spyware, and Vulnerability Protection profiles associated with each rule determine which threats are logged (locally or remotely). To apply logging profiles to security policies, refer to “Defining Security Policies”.

On a PA-7000 Series firewalls, a special interface type (Log Card) must be configured before the firewall will forward the following log types: Syslog, Email, and SNMP. This is also required to forward files to WildFire. After the port is configured, log forwarding and WildFire forwarding will automatically use this port and there is no special configuration required for this to occur. Just configure a data port on one of the PA-7000 Series NPCs as interface type Log Card and ensure that the network that will be used can communicate with your log servers. For WildFire forwarding, the network will need to communicate with the WildFire cloud and/or WildFire appliance.

For information on configuring this interface, see “Configure a Log Card Interface”.

The following table describes the log forwarding settings:

Table 169. Log Forwarding Profile Settings

Field	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.
Shared	Select this check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Traffic Settings	
Panorama	Select the check box to enable sending traffic log entries to the Panorama centralized management system. To define the Panorama server address, refer to “Defining Management Settings”.

Table 169. Log Forwarding Profile Settings (Continued)

Field	Description
SNMP Trap Email Syslog	Select the SNMP, syslog, and/or email settings that specify additional destinations where the traffic log entries are sent. To define new destinations, refer to: • "Configuring SNMP Trap Destinations". • "Configuring Email Notification Settings" • "Configuring Syslog Servers"
Threat Log Settings	
Panorama	Click the check box for each severity level of the threat log entries to be sent to Panorama. The severity levels are: • **Critical**—Very serious attacks detected by the threat security engine. • **High**—Major attacks detected by the threat security engine. • **Medium**—Minor attacks detected by the threat security engine. • **Low**—Warning-level attacks detected by the threat security engine. • **Informational**—All other events including URL blocking and informational attack object matches that are not covered by the other severity levels.
SNMP Trap Email Syslog	Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the threat log entries are sent.

Decryption Profiles

▶ *Objects > Decryption Profile*

Decryption profiles enable you to block and control specific aspects of the SSL forward proxy, SSL inbound inspection, and SSH traffic. After you create a decryption profile, you can then add that profile to a decryption policy; any traffic matched to the decryption policy will be enforced according to the profile settings.

You can also control the trusted CAs that your device trusts, for more information, refer to "Managing the Default Trusted Certificate Authorities".

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.

The following sections provide descriptions for settings that are commonly applied to traffic matched to a decryption policy, as well as details for settings that can be applied specifically to decrypted SSL traffic, decrypted SSH traffic, and traffic that is matched to a No Decrypt policy (decryption exceptions):

- "Decryption Profile General Settings"
- "SSL Decryption Settings in a Decryption Profile"
- "No Decryption Settings in a Decryption Profile"
- "SSH Proxy Settings in a Decryption Profile"

Before you can enable decryption port mirroring, you must obtain a Decryption Port Mirror license, install the license, and reboot the firewall.

Table 170. Decryption Profile General Settings

Field	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	Select this check box if you want the profile to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the profile will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the profile will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Decryption Mirroring Interface (PA-3000 Series, PA-5000 Series, and PA-7000 Series firewalls only)	Select an **Interface** to use for decryption port mirroring.
Forwarded Only (PA-3000 Series, PA-5000 Series, and PA-7000 Series firewalls only)	Select the **Forwarded Only** check box 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 the check box (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.
SSL Decryption, No Decryption, and SSH Proxy tabs	For details on additional profile settings for SSL Decryption, No Decryption, and SSH Proxy, see: • "SSL Decryption Tab Settings" • "No Decryption Tab Settings" • "SSH Proxy Tab Settings"

SSL Decryption Settings in a Decryption Profile

The following table describes the settings you can use to control SSL traffic that has been decrypted using either SSL Forward Proxy decryption or SSL Inbound Inspection. You can use these settings to limit or block SSL 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.

Table 171. SSL Decryption Tab Settings

Field	Description
SSL Forward Proxy Subtab	With SSL Forward Proxy decryption, the firewall functions as a proxy to a session between an internal client and outside server, generating a forward trust (or forward untrust, if the original server certificate is not signed by a trusted CA) certificate for the external server that is then presented to the client. The firewall is established as a trusted third party to the session. Select options to limit or block SSL traffic decrypted using SSL Forward Proxy.
Server Certificate Validation	Select options to control server certificates for decrypted SSL traffic.
Block sessions with expired certificates	Terminate the SSL connection if the server certificate is expired. This will prevent a user from being able to accept an expired certificate and continuing with an SSL session.
Block sessions with untrusted issuers	Terminate the SSL session if the server certificate issuer is untrusted.
Block sessions with unknown certificate status	Terminate the SSL 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 on the certificate status check timeout	Terminate the SSL 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**).
Restrict certificate extensions	Limits the certificate extensions used in the dynamic server certificate to key usage and extended key usage.
Unsupported Mode Checks	Select options to control unsupported SSL applications.
Block sessions with unsupported version	Terminate sessions if PAN-OS does not support the “client hello” message. PAN-OS supports SSLv3, TLS1.0, TLS1.1, and TLS1.2.
Block sessions with unsupported cipher suites	Terminate the session if the cipher suite specified in the SSL handshake if it is not supported by PAN-OS.
Block sessions with client authentication	Terminate sessions with client authentication for SSL forward proxy traffic.
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.
Block sessions if HSM not available	Terminate sessions if a hardware security module (HSM) is not available to sign certificates.
Note: *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. Use the check boxes to block those sessions instead.*	

Table 171. SSL Decryption Tab Settings (Continued)

Field	Description
SSL Inbound Inspection Subtab	With SSL Inbound Inspection, the firewall resides between a client and a targeted server, where the targeted server certificate and key is imported to the firewall. This allows the firewall to access the SSL session between the targeted server and the client transparently, rather than functioning as a proxy (as with SSL Forward Proxy decryption). Select options to limit or block SSL traffic decrypted using SSL Forward Proxy.
Unsupported Mode Checks	Select options to control sessions if unsupported modes are detected in SSL traffic.
Block sessions with unsupported versions	Terminate sessions if PAN-OS does not support the “client hello” message. PAN-OS supports SSLv3, TLS1.0, TLS1.1, and TLS1.2.
Block sessions with unsupported cipher suites	Terminate the session if the cipher suite used is not supported by PAN-OS.
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.
Block sessions if HSM not available	Terminate sessions if a hardware security module (HSM) is not available to decrypt the session key.
SSL Protocol Settings Subtab	Select the following settings to enforce protocol versions and cipher suites for SSL session traffic.
Protocol Versions	Enforce the use of minimum and maximum protocol versions for the SSL session.
Min Version	Set the minimum protocol version that can be used to establish the SSL connection.
Max Version	Set the maximum protocol version that can be used to establish the SSL 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.
Encryption Algorithms	Enforce the use of the selected encryption algorithms for the SSL session.
Authentication Algorithms	Enforce the use of the selected authentication algorithms for the SSL session.

No Decryption Settings in a Decryption Profile

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.

Table 172. No Decryption Tab Settings

Field	Description
Block sessions with expired certificates	Terminate the SSL connection if the server certificate is expired. This will prevent a user from being able to accept an expired certificate and continuing with an SSL session.
Block sessions with untrusted issuers	Terminate the SSL session if the server certificate issuer is untrusted.

SSH Proxy Settings in a Decryption Profile

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.

Table 173. SSH Proxy Tab Settings

Field	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.
Block sessions with unsupported algorithms	Terminate sessions if the algorithm specified by the client or server is not supported by PAN-OS.
Failure Checks	*Select actions to take if SSH application errors occur and if system resources are not available.*
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.

Schedules

▶ *Objects > Schedules*

By default, each security policy applies to all dates and times. To limit a security policy 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 “Defining Security Policies”.

When a security policy is invoked by a defined schedule, only new sessions are affected by the applied security policy. Existing sessions are not affected by the scheduled policy.

The following table describes the schedule settings:

Table 174. Schedule Settings

Field	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	Select this check box if you want the schedule to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear the check box, the schedule will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear the check box, the schedule will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select the check box if you want to prevent administrators from creating local copies of the schedule in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Recurrence	Select the type of schedule (**Daily**, **Weekly**, or **Non-Recurring**).
Daily	Click **Add** and specify a start and end time in 24-hour format (HH:MM).
Weekly	Click **Add**, select a day of the week, and specify the start and end time in 24-hour format (HH:MM).
Non-recurring	Click **Add** and specify a start and end date and time.

Chapter 6
Reports and Logs

The following topics describe how to use the dashboard, Application Command Center (ACC), reports, and logs on the firewall to monitor activity on your network:

- "Using the Dashboard"
- "Using the Application Command Center"
- "Using App Scope"
- "Viewing the Logs"
- "Using the Automated Correlation Engine"
- "Working with Botnet Reports"
- "Managing PDF Summary Reports"
- "Managing User/Group Activity Reports"
- "Managing Report Groups"
- "Scheduling Reports for Email Delivery"
- "Viewing Reports"
- "Generating Custom Reports"
- "Taking Packet Captures"

Most of the reports in this section support optional selection of a virtual system from the drop-down list at the top of page.

Using the Dashboard

▶ *Dashboard*

The **Dashboard** page Widgets show general device information, such as the software version, the operational status of each interface, resource utilization, and up to 10 entries in the threat, configuration, and system logs. Log entries from the last 60 minutes are displayed. All of the available Widgets are displayed by default, but each user can remove and add individual Widgets, as needed.

Click the refresh icon ⟳ to update the Dashboard or an individual widget. To change the automatic refresh interval, select an interval from the drop-down list (1 min, 2 mins, 5 mins, or Manual). To add a Widget to the Dashboard, click the Widget drop-down, select a category and then the widget name. To delete a widget, click ✕ in the title bar.

Table 175. Dashboard Charts

Chart	Description
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.
General Information	Displays the device name, model, PAN-OS® software version, the application, threat, and URL filtering definition versions, the current date and time, and the length of time since the last restart.
Interface Status	Indicates whether each interface is up (green), down (red), or in an unknown state (gray).
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. Only entries from last 60 minutes are displayed.
Config Logs	Displays the administrator user name, client (Web or CLI), and date and time for the last 10 entries in the Configuration log. Only entries from the last 60 minutes are displayed.
Data Filtering Logs	Displays the description and date and time for the last 60 minutes in the Data Filtering log.
URL Filtering Logs	Displays the description and date and time for the last 60 minutes in the URL Filtering log.
System Logs	Displays the description and date and time for the last 10 entries in the System log. Note that a "Config installed" entry indicates configuration changes were committed successfully. Only entries from the last 60 minutes are displayed.

Table 175. Dashboard Charts (Continued)

Chart	Description
System Resources	Displays the Management CPU usage, Data Plane usage, and the Session Count, which displays the number of sessions established through the firewall.
Logged In Admins	Displays the source IP address, session type (Web or CLI), and session start time for each administrator who is currently logged in.
ACC Risk Factor	Displays the average risk factor (1 to 5) for the network traffic processed over the past week. Higher values indicate higher risk.
High Availability	If high availability (HA) is enabled, indicates the HA status of the local and peer device—green (active), yellow (passive), or black (other). For more information about HA, refer to “Enabling HA on the Firewall”.
Locks	Shows configuration locks taken by administrators.

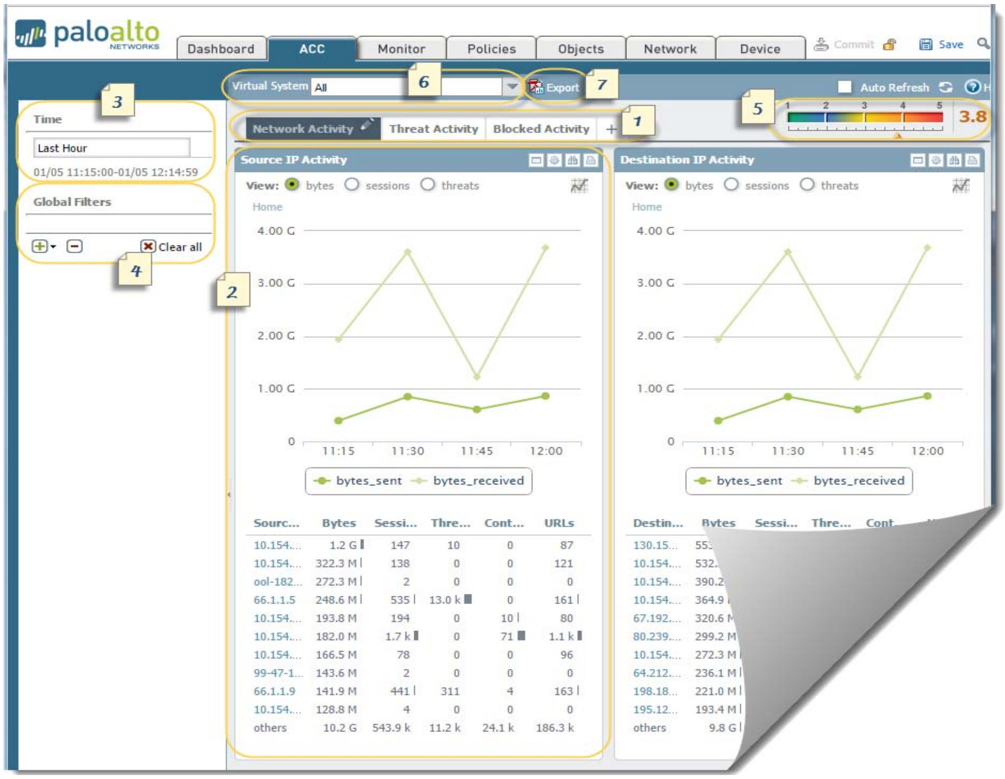
Using the Application Command Center

- *ACC*

The Application Command Center (ACC) is an analytical tool that provides actionable intelligence on activity within your network. The ACC uses the firewall logs for graphically depicting 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.

What do you want to know?	See
How do I use the ACC?	▶ *"A First Glance at the ACC"* ▶ *"Views"* ▶ *"Widgets"*
How do I interact with the ACC?	▶ *"Actions"* ▶ *"Working with Filters"*
Do you want more? Can't find what you're looking for?	**See** Use the Application Command Center

A First Glance at the ACC



Sourc...	Bytes	Sessi...	Thre...	Cont...	URLs
10.154....	1.2 G	147	10	0	87
10.154....	322.3 M	138	0	0	121
ool-182...	272.3 M	2	0	0	0
66.1.1.5	248.6 M	535	13.0 k	0	161
10.154....	193.8 M	194	0	10	80
10.154....	182.0 M	1.7 k	0	71	1.1 k
10.154....	166.5 M	78	0	0	96
99-47-1...	143.6 M	2	0	0	0
66.1.1.9	141.9 M	441	311	4	163
10.154....	128.8 M	4	0	0	0
others	10.2 G	543.9 k	11.2 k	24.1 k	186.3 k

Destin...	Bytes	Sessi...	Thre...	Cont
130.15...	55			
10.154....	532.			
10.154....	390.2			
10.154....	364.9			
67.192....	320.6 M			
80.239....	299.2 M			
10.154....	272.3 M			
64.212....	236.1 M			
198.18...	221.0 M			
195.12...	193.4 M			
others	9.8 G			

1 **Tabs** The ACC includes three predefined tabs or views that provide visibility into network traffic, threat activity, and blocked activity. For information on each view, see “Views”.

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, threats (malicious and benign), and count. For information on each widget, see “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 30 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:

01/12 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 “Actions”.

5 **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.

A First Glance at the ACC		
6	**Source**	The data source used for the display varies between the firewall and Panorama™. On the firewall, if 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. On Panorama, you can change the display to use **Panorama** or **Remote Device Data**. When the data source is Panorama, you can filter the display for a specific device group.
7	**Export**	You can export the widgets displayed in the current tab as a PDF.

Views

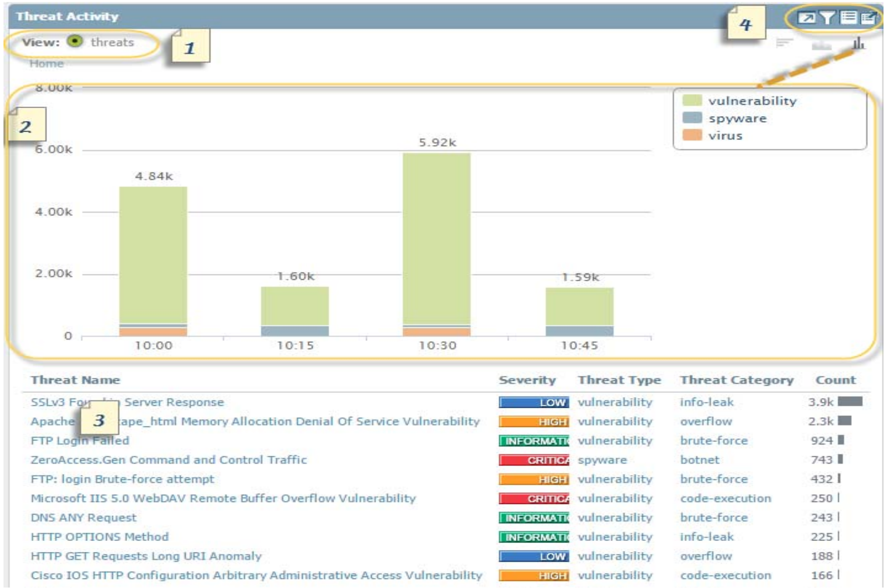
- **Network Activity**—This tab displays an overview of traffic and user activity on your network. It focuses on the top applications being used, the top users who generate traffic with a drill down into the bytes, content, threats or URLs accessed by the user, and the most used security rules against which traffic matches occur. In addition, you can also 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**—This tab 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 (**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**—This tab 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, user name, threat name, content (files and data), and the top security rules with a deny action that blocked traffic.

Widgets

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



Threat Name	Severity	Threat Type	Threat Category	Count
SSLv3 Fo[illegible] Server Response	LOW	vulnerability	info-leak	3.9k
Apache [illegible]ape_html Memory Allocation Denial Of Service Vulnerability	HIGH	vulnerability	overflow	2.3k
FTP Login Failed	INFORMATI	vulnerability	brute-force	924
ZeroAccess.Gen Command and Control Traffic	CRITICA	spyware	botnet	743
FTP: login Brute-force attempt	HIGH	vulnerability	brute-force	432
Microsoft IIS 5.0 WebDAV Remote Buffer Overflow Vulnerability	CRITICA	vulnerability	code-execution	250
DNS ANY Request	INFORMATI	vulnerability	brute-force	243
HTTP OPTIONS Method	INFORMATI	vulnerability	info-leak	225
HTTP GET Requests Long URI Anomaly	LOW	vulnerability	overflow	188
Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	HIGH	vulnerability	code-execution	166

Each widget is structured to display the following:

1	**View**	You can sort the data by bytes, sessions, threats, count, content, URLs, malicious, benign, files, data, profiles, objects. 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, and map. The available options vary by widget; the interaction experience also 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 into the graph. The area you click on becomes a filter and allows you to zoom in to the selection and view more granular information for that selection.

3	**Table**	The detailed view of the data used to render the graph is provided 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 only display information that pertains to your filter.
4	**Actions**	**Maximize view**— Allows you enlarge the widget and view it in a larger screen space. In the maximized view, you can see more than the top ten items displayed in the default screen width for the widget. **Set up local filters**—Allows you to add filters to 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*** tab). The logs are filtered using the time period for which the graph is rendered. If you have 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.

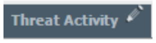
For a description of each widget, see the details on using the ACC.

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

Working with Tabs and Widgets	
• Add a tab.	1. Select the + icon 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 5 tabs.
• Edit a tab.	1. Select the tab, and click the pencil icon next to the tab name, to edit the tab. For example  Threat Activity .
• See what the widgets are included in a view.	1. Select the view, and click on the pencil icon to edit the view. 2. Select the **Add Widgets** drop-down and verify the widgets that have the check boxes enabled.
• 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 check box that corresponds to the widget you want to add. You can select up to a maximum of 12 widgets. 3. (Optional) To create a 2-column layout, select **Add Widget Group**. You can drag and drop widgets into the 2-column display. As you drag the widget into the layout, a placeholder will display for you to drop the widget. **Note:** *You cannot name a widget group.*
• Delete a tab or a widget group/ widget.	1. To delete a custom tab, select the tab and click the X icon. **Note:** *You cannot delete a predefined tab.* 2. To delete a widget group/widget, edit the tab and then click the [X] icon on the right. *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 click **Reset View**.

Working with Filters— Local Filters and Global Filters

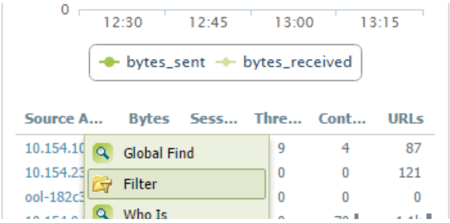
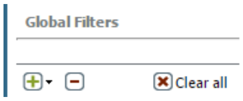
In order to hone in to the details and finely control what the ACC displays, you can use filters.

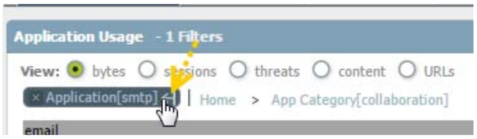
Local Filters: Local filters are applied on a specific widget. A local filter allows you to interact with the graph and customize the display so that you can dig in to the details and access the information you want to monitor on a specific widget. You can apply a local filter in two ways—clicking into an attribute in the graph or table, or by using the Set Filter icon ▽within a widget. The Set Filter icon 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 about right now 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 the application as a global filter and view only information pertaining to that user and application through all the tabs and widgets on the ACC. Global filters are not persistent.

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.
- **Promote a local filter for use as a global filter:** This option allows you to promote an attribute that you have set as a local filter to be a global filter. Promoting a local to a global filter changes the display across all views on the ACC.
- **Define a global filter:** Define a filter using the **Global Filters** pane on the ACC.

Working with Filters	
• Set a local filter. **Note:** *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 the ▽ icon. 2. Click the ⊞ icon to add the filters you want to apply. 3. Click **Apply**. These filters are persistent across reboots. **Note:** *The number of local filters applied on a widget are indicated next to the widget name.*
• Set a global filter from a table.	1. Hover over an attribute in the table below the chart, and click the drop down. 2. Click **Filter** to add the attribute as a global filter.  0 12:30 12:45 13:00 13:15 bytes_sent bytes_received Source A... Bytes Sess... Thre... Cont... URLs 10.154.10 9 4 87 10.154.23 0 0 121 ool-182c3 0 0 0
• Set a global filter using the Global Filters pane  Global Filters ⊞▾ ⊟ ☒ Clear all	Click the ⊞ icon to add the filters you want to apply.

Working with Filters	
• Promote a local filter to as global filter.	1. On any table in a widget, click the link for an attribute. This sets the attribute as a local filter. 2. To promote the filter to be a global filter, select the arrow to the left of the filter.  Application Usage - 1 Filters View: ● bytes ○ sessions ○ threats ○ content ○ URLs × Application[smtp] Home > App Category[collaboration] email
• Remove a filter.	Click the ⊟ icon to remove a filter. • For global filters: It is located in the Global Filters pane. • For local filters: Click the ▽ icon to bring up the Setup Local Filters dialog, then select the filter and click the delete icon.
• Clear all filters	• For global filters: Click the **Clear All** button under Global Filters. • For local filters: Select a widget and click the ▽ icon. Then click the **Clear All** button in the Setup Local Filters widget.
• Negate filters	Select an attribute and click the ⊘ icon to negate a filter. • For global filters: It is located in the Global Filters pane. • For local filters: Click the ▽ icon to bring up the Setup Local Filters dialog, add a filter and then click the negate icon.
• View what filters are in use.	• For global filters: The number of global filters applied are displayed on the left pane under Global Filters. • For local filters: The number of local filters applied on a widget are displayed next to the widget name. To view the filters, click the **Set Local Filters** icon.

Using App Scope

▶ *Monitor > App Scope*

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, that stores logs forwarded by the managed devices; on an upgrade the default data source is the remote device data. To fetch and display an aggregated view of the data directly from the managed devices, 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.

Table 176. Application Command Center Charts

Chart	Description
Summary	"Summary Report"
Change Monitor	"Change Monitor Report"
Threat Monitor	"Threat Monitor Report"
Threat Map	"Threat Map Report"
Network Monitor	"Network Monitor Report"
Traffic Map	"Traffic Map Report"

Summary Report

The Summary report (Figure 7) 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.

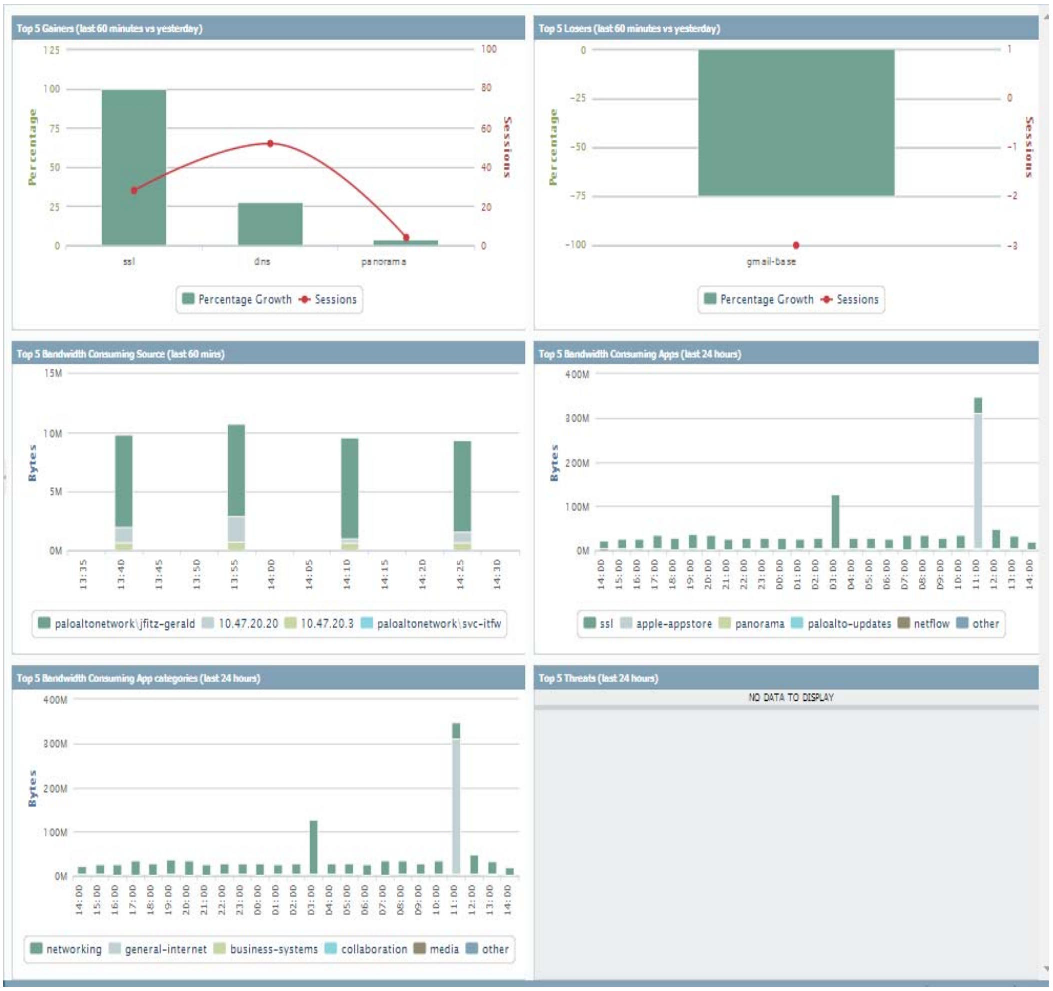
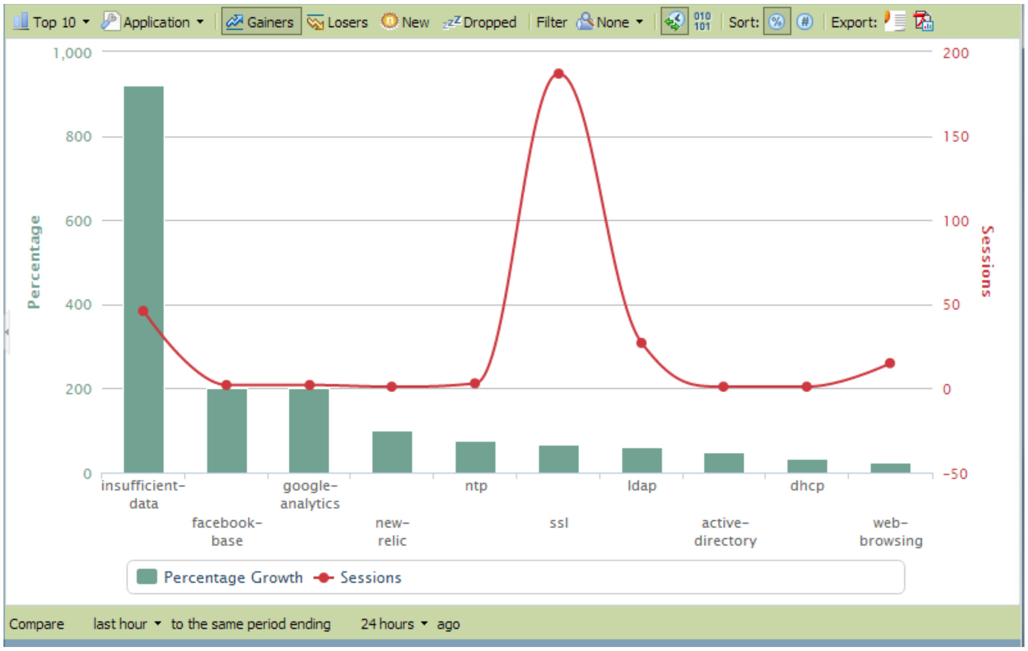


Figure 7. App Scope Summary Report

Change Monitor Report

The Change Monitor report (Figure 8) displays changes over a specified time period. For example, Figure 8 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.

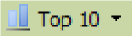
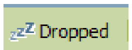
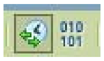
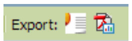
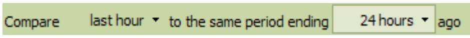


Compare last hour to the same period ending 24 hours ago

Figure 8. App Scope Change Monitor Report

This report contains the following buttons and options.

Table 177. Change Monitor Report Options

Item	Description
Top Bar	
	Determines the number of records with the highest measurement included in the chart.
	Determines the type of item reported: Application, Application Category, Source, or Destination.
	Displays measurements of items that have increased over the measured period.
	Displays measurements of items that have decreased over the measured period.
	Displays measurements of items that were added over the measure period.
	Displays measurements of items that were discontinued over the measure period.
	Applies a filter to display only the selected item. **None** displays all entries.
	Determines whether to display session or byte information.
	Determines whether to sort entries by percentage or raw growth.
	Exports the graph as a .png image or as a PDF.
Bottom Bar	
	Specifies the period over which the change measurements are taken.

Threat Monitor Report

The Threat Monitor report (Figure 9) displays a count of the top threats over the selected time period. For example, Figure 9 shows the top 10 threat types for the past 6 hours.

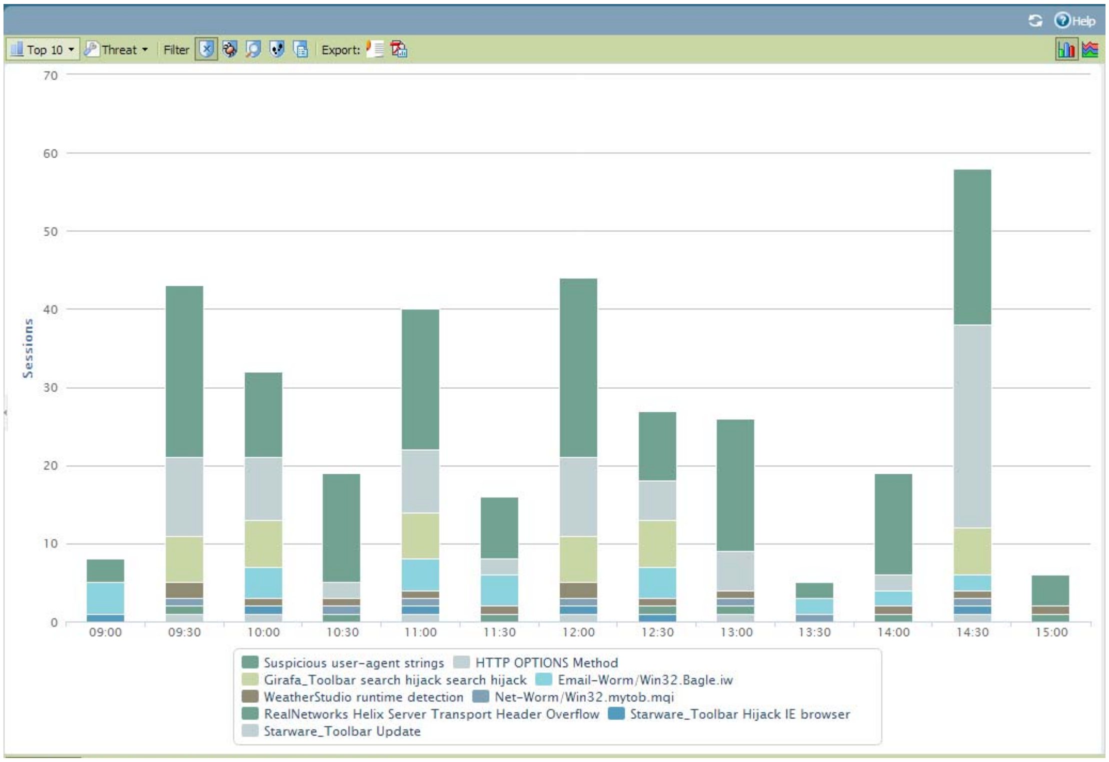
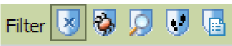
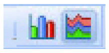
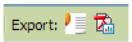

Help
Top 10
Threat
Filter
Export:
Sessions
70
60
50
40
30
20
10
0
09:00
09:30
10:00
10:30
11:00
11:30
12:00
12:30
13:00
13:30
14:00
14:30
15:00
Suspicious user-agent strings
HTTP OPTIONS Method
Girafa_Toolbar search hijack search hijack
Email-Worm/Win32.Bagle.iw
WeatherStudio runtime detection
Net-Worm/Win32.mytob.mqi
RealNetworks Helix Server Transport Header Overflow
Starware_Toolbar Hijack IE browser
Starware_Toolbar Update

Figure 9. App Scope Threat Monitor Report

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

Table 178. Threat Monitor Report Buttons

Button	Description
Top Bar	
Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
Threats ▾	Determines the type of item measured: Threat, Threat Category, Source, or Destination.
 Filter	Applies a filter to display only the selected type of items.
	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	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Specifies the period over which the measurements are taken.

Threat Map Report

The Threat Map report (Figure 10) shows a geographical view of threats, including severity.

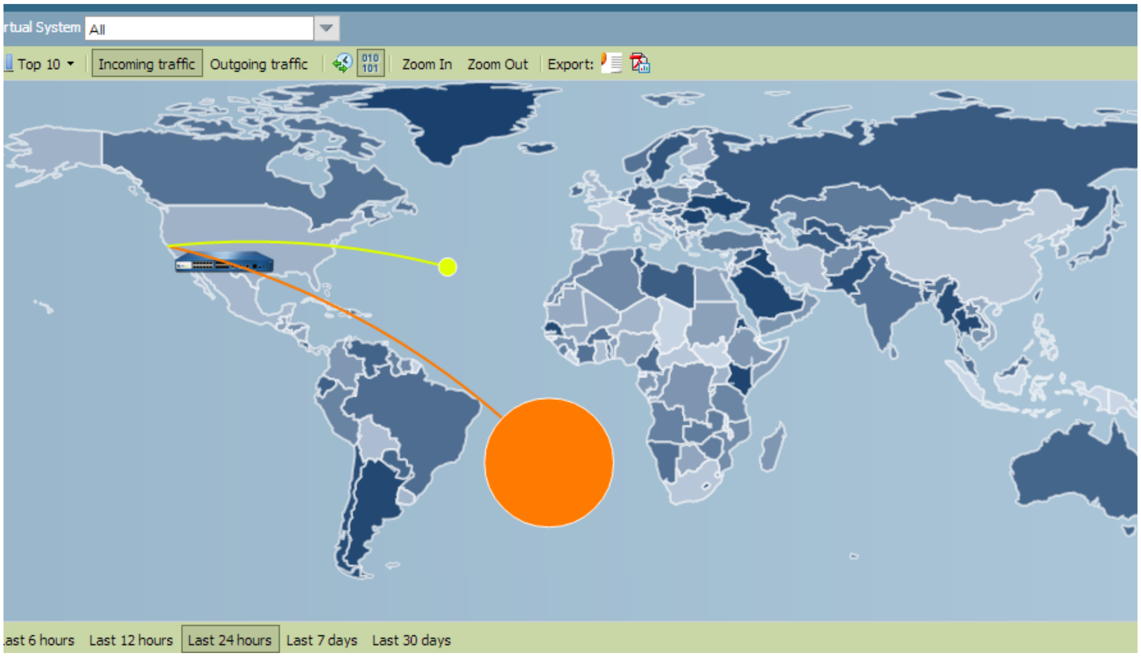
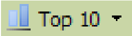
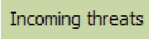
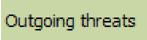
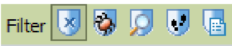
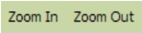
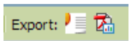
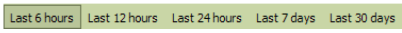


Figure 10. App Scope Threat Map Report

Each threat type is color-coded as indicated in the legend below the chart. Click a country on the map to zoom in. Click the **Zoom Out** button in the lower right corner of the screen to zoom out. This report contains the following buttons and options.

Table 179. Threat Map Report Buttons

Button	Description
Top Bar	
	Determines the number of records with the highest measurement included in the chart.
	Displays incoming threats.
	Displays outgoing threats.
	Applies a filter to display only the selected type of items.
	Zoom in and zoom out of the map.
	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	Indicates the period over which the measurements are taken.

Network Monitor Report

The Network Monitor report (Figure 11) 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, Figure 11 shows application bandwidth for the past 7 days based on session information.

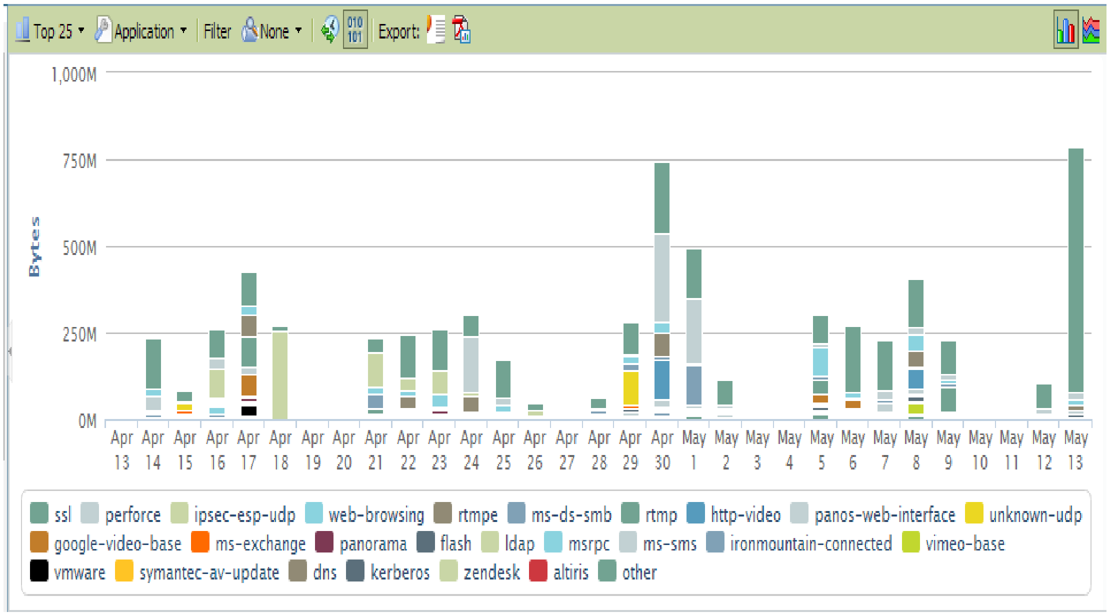


Figure 11. App Scope Network Monitor Report

The report contains the following buttons and options.

Table 180. Network Monitor Report Buttons

Button	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 None ▾	Applies a filter to display only the selected item. **None** displays all entries.
010 101	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	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indicates the period over which the change measurements are taken.

Traffic Map Report

The Traffic Map report (Figure 12) shows a geographical view of traffic flows according to sessions or flows.

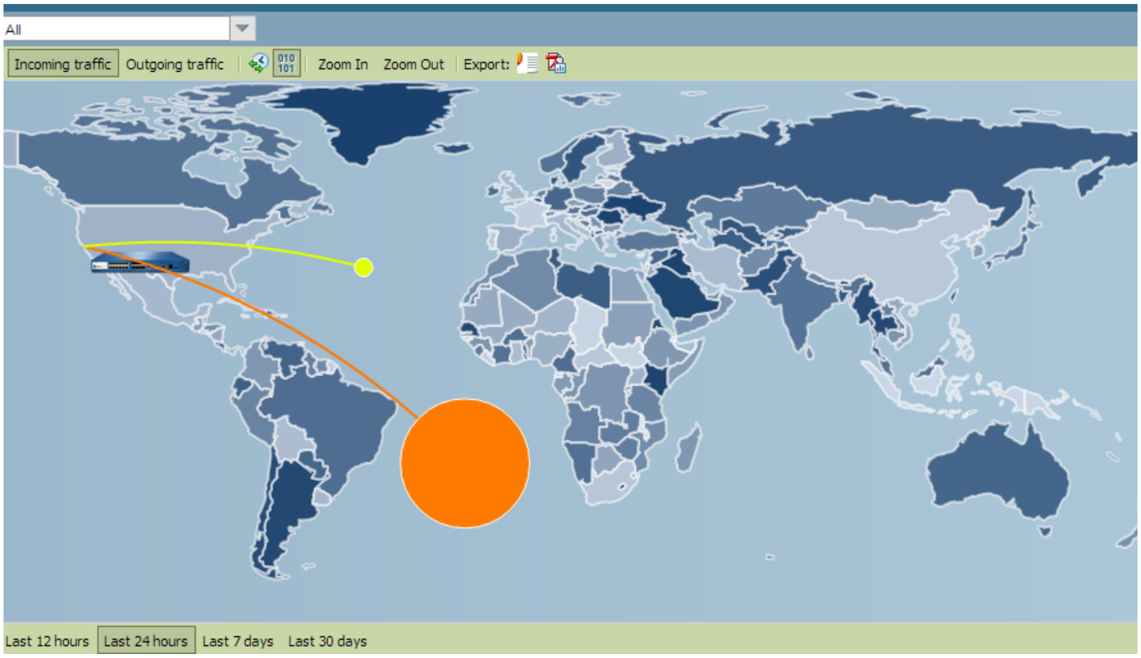
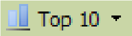
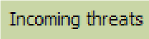
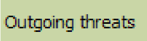
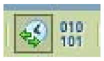
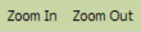
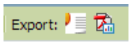
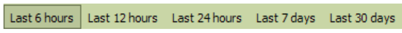


Figure 12. App Scope Traffic Map Report

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

Table 181. Threat Map Report Buttons

Button	Description
Top Bar	
 Top 10	Determines the number of records with the highest measurement included in the chart.
 Incoming threats	Displays incoming threats.
 Outgoing threats	Displays outgoing threats.
 010 101	Determines whether to display session or byte information.
 Zoom In 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	Indicates the period over which the change measurements are taken.

Viewing the Logs

▶ *Monitor > Logs*

The firewall maintains logs for WildFire, configurations, system, alarms, traffic flows, threats, URL filtering, data filtering, and Host Information Profile (HIP) matches. You can view the current logs at any time. To locate specific entries, you can apply filters to most of the log fields.

The firewall displays the information in logs so that role-based administration permissions are respected. When you display logs, only the information that you have permission to see is included. For information on administrator permissions, refer to "Defining Administrator Roles".

To view the logs, click the log types on the left side of the page in the **Monitor** tab.

Table 182. Log Descriptions

Chart	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. Click 🔍 next to an entry 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). Note that 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”.
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, and the alarm action (allow or block) and severity. Click 🔍 next to an entry 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). Note that 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. If local packet captures are enabled, click ⬇ next to an entry to access the captured packets, as in the following figure. To enable local packet captures, refer to the subsections under “Security Profiles”.
URL Filtering	Displays logs for URL filters, which block access to specific web sites and web site categories or generate an alert when a web site is accessed. You can enable logging of the HTTP header options for the URL. Refer to “URL Filtering Profiles” for information on defining URL filtering profiles.
WildFire Submissions	Displays logs for files that are uploaded and analyzed by the WildFire server, log data is sent back to the device after analysis, along with the analysis results.
Data Filtering	Displays logs for the security policies that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall. Refer to “Data Filtering Profiles” for information on defining data filtering profiles. To configure password protection for access the details for a log entry, click the ⬇ icon. Enter the password and click **OK**. Refer to “Defining Custom Response Pages” for instructions on changing or deleting the data protection password. **Note:** *The system prompts you to enter the password only once per session.* This log also shows information for file blocking profiles. For example, if you are blocking .exe files, the log will show that the files that were blocked. If you forward files to WildFire, you will see the results of that action. In this case, if you are forwarding PE files to WildFire for example, the log will show that the file was forwarded and will also show the status on whether or not it was uploaded to WildFire successfully or not.

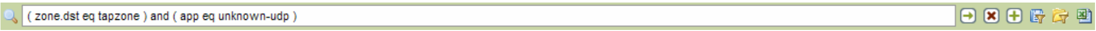
Table 182. Log Descriptions (Continued)

Chart	Description
Configuration	Displays an entry for each configuration change. Each entry includes the date and time, the administrator user name, the IP address from where the change was made, the type of client (Web 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.
HIP Match	Displays information about security policies that apply to GlobalProtect™ clients. For more information, refer to “Setting Up the GlobalProtect Portal”.
Alarms	The alarms log records detailed information on alarms that are generated by the system. The information in this log is also reported in the **Alarms** window. Refer to “Defining Alarm Settings”.

Interacting with Logs

- **Use the filters**: Filters allow you to parse the log files according to your needs. You can, for example, just view logs for a specific attribute such as an IP address within a specific time range.

  Each log page has a filter area at the top of the page.



(zone.dst eq tapzone) and (app eq unknown-udp)

  – Click any of the underlined links in the log listing to add that item as a log filter option. For example, if you click the **Host** link in the log entry for 10.0.0.252 and **Web Browsing** in both items are added, and the search will find entries that match both (AND search).

  – To define other search criteria, click the **Add Log Filter** icon. Select the type of search (and/or), the attribute to include in the search, the matching operator, and the values for the match, if appropriate. Click **Add** to add the criterion to the filter area on the log page, and then click **Close** to close the pop-up window. Click the **Apply Filter** icon to display the filtered list.

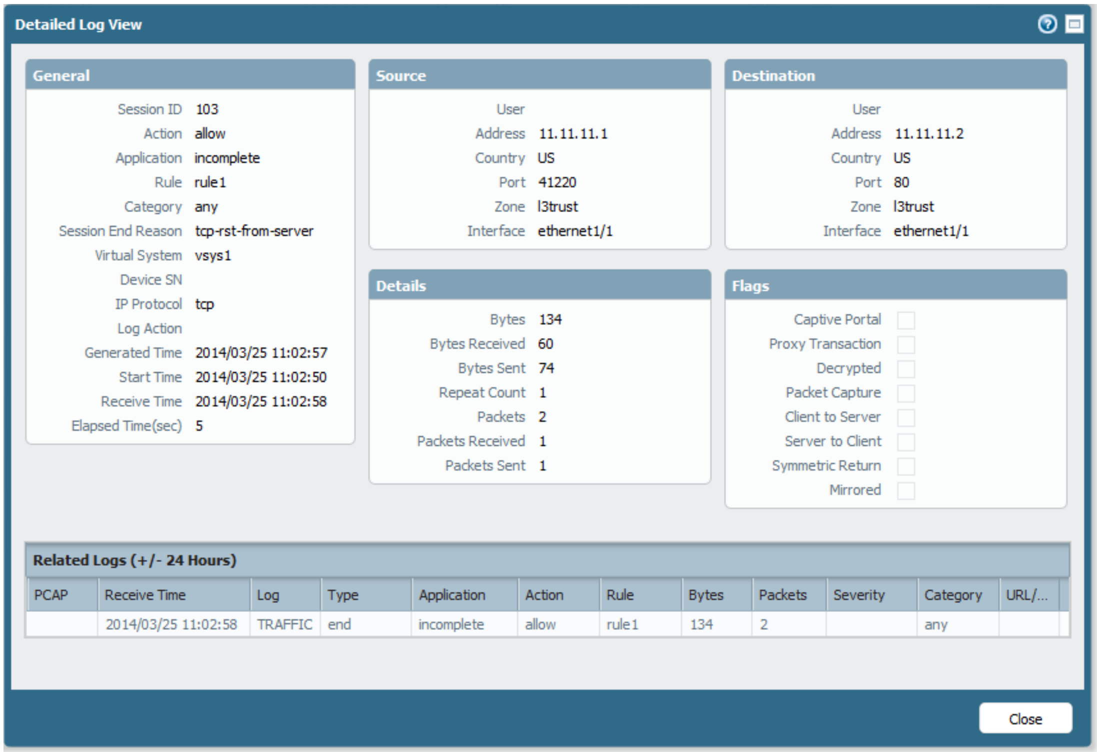
If the **Value** *string matches an* **Operator** *(such as* **has** *or* **in***), enclose the string in quotation marks to avoid a syntax error. For example, if you filter by destination country and use* `IN` *as a* **Value** *to specify INDIA, enter the filter as* `( dstloc eq "IN" )`*.*

You can combine filter expressions added on the log page with those you define in the Add Log Filter dialog. The filter field on the log page displays each filter as an entry.

If you add a **Receive Time** *filter with the* **Operator** *set to* **in** *and the* **Value** *set to* **Last 60 seconds***, some of the page links on the log viewer might not show results because the number of pages might grow or shrink due to the dynamic nature of the selected time.*

- To clear filters and redisplay the unfiltered list, click the **Clear Filter** button.
- To save your selections as a new filter, click the **Save Filter** button, enter a name for the filter, and click **OK**.
- To export the current log listing (as shown on the page, including any applied filters) click the **Save Filter** button. Select whether to open the file or save it to disk, and select the check box if you want to always use the same option. Click **OK**.

- **Export logs**: To export the current log listing in CSV format, select the Export to CSV icon . By default, exporting the log listing to CSV format will generate a CSV report with up to 2,000 lines of logs. To change the line limit for generated CSV reports, use the **Max Rows in CSV Export** field (select **Device > Setup > Management > Logging and Reporting Settings > Log Export and Reporting** or refer to “Defining Management Settings”).
- **Change the automatic refresh interval**: Select an interval from the drop-down (**1 min**, **30 seconds**, **10 seconds**, or **Manual**).
- **Change the 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 **Rows** drop-down. To sort the results in ascending or descending order, use the **ASC** or **DESC** drop-down.
- **Resolve IP addresses to domain names**: Select the **Resolve Hostname** check box to begin resolving external IP addresses to domain names.
- **View additional log details**: To display additional details, click the spyglass icon for an entry.



Detailed Log View

General

Session ID	103
Action	allow
Application	incomplete
Rule	rule1
Category	any
Session End Reason	tcp-rst-from-server
Virtual System	vsys1
Device SN	
IP Protocol	tcp
Log Action	
Generated Time	2014/03/25 11:02:57
Start Time	2014/03/25 11:02:50
Receive Time	2014/03/25 11:02:58
Elapsed Time(sec)	5

Source

User	
Address	11.11.11.1
Country	US
Port	41220
Zone	l3trust
Interface	ethernet1/1

Destination

User	
Address	11.11.11.2
Country	US
Port	80
Zone	l3trust
Interface	ethernet1/1

Details

Bytes	134
Bytes Received	60
Bytes Sent	74
Repeat Count	1
Packets	2
Packets Received	1
Packets Sent	1

Flags

Captive Portal	□
Proxy Transaction	□
Decrypted	□
Packet Capture	□
Client to Server	□
Server to Client	□
Symmetric Return	□
Mirrored	□

Related Logs (+/- 24 Hours)

PCAP	Receive Time	Log	Type	Application	Action	Rule	Bytes	Packets	Severity	Category	URL/...
	2014/03/25 11:02:58	TRAFFIC	end	incomplete	allow	rule1	134	2		any	

If the source or destination has an IP address to name 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.

Viewing Session Information

▶ *Monitor > Session Browser*

Open the **Session Browser** page to browse and filter current running sessions on the firewall. For information on filtering options for this page, refer to “Viewing the Logs”.

Using the 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 automated correlation engine is supported on the following platforms only:

- Panorama—M-Series and the virtual appliance
- PA-3000 Series firewalls
- PA-5000 Series firewalls
- PA-7000 Series firewalls

What do you want to know?	**See**
What are correlation objects?	▶ *"View the Correlation Objects"*
What is a correlated event? Where do I see the match evidence for a correlation match?	▶ *"View the Correlated Events"*
How can I see a graphical view of correlation matches?	▶ *See the Compromised Hosts widget in "Using the Application Command Center".*
Do you want more? Can't find what you're looking for?	**See** Use the Automated Correlation Engine

View the Correlation Objects

▶ *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.

A correlation object includes the following fields:

Field	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.

By default, all correlation objects are enabled. To disable an object, select the check box next to the object and click **Disable**.

View the Correlated Events

▶ *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 following details:

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.

To view additional details, click the detailed log view for an entry. The detailed log view includes all the evidence on a match:

Tab	Description
Match Information	Object Details: Presents information on the correlation object that triggered the match. For information on correlation objects, see "View the 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.

Working with Botnet Reports

The botnet report enables you to use behavior-based mechanisms to identify potential 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 specify types of traffic as suspicious. The PAN-OS Administrator's Guide provides details on interpreting botnet report output.

- "Managing Botnet Reports"
- "Configuring the Botnet Report"

Managing Botnet Reports

▶ *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** on the right side of the page and complete the following fields. To export a report, select it and click **Export to PDF**, **Export to CSV**, or **Export to XML**.

Table 183. Botnet Report Settings

Field	Description
Test Run Time Frame	Select the time interval for the report: **Last 24 Hours** (the default) or **Last Calendar Day**.
Run Now	Click the button to manually generate the report immediately. The dialog displays the report in a new tab.
No. of Rows	Specify the number of rows in the report (default is 100).
Scheduled	Select the check box to automatically generate the report daily. By default, the check box is enabled.
Query Builder	For each query that you want the report to run, complete the following fields and click **Add**. • **Connector**—Select a logical connector (**and**/**or**). Selecting the **Negate** check box applies negation to the query: 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.

Configuring the Botnet Report

▶ *Monitor > Botnet*

To specify the types of traffic that indicate potential botnet activity, click the **Configuration** button 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 “Managing Botnet Reports”).

Table 184. Botnet Configuration Settings

Field	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**—Identifies users communicating with known malware URLs based on malware and botnet URL filtering categories. • **Use of dynamic DNS**—Looks for traffic that is destined for dynamic DNS sites, which might indicate botnet communication. • **Browsing to IP domains**—Identifies users who browse to IP domains instead of URLs. • **Browsing to recently registered domains**—Looks for traffic to domains that were registered within the past 30 days. • **Executable files from unknown sites**—Identifies executable files downloaded from unknown URLs.

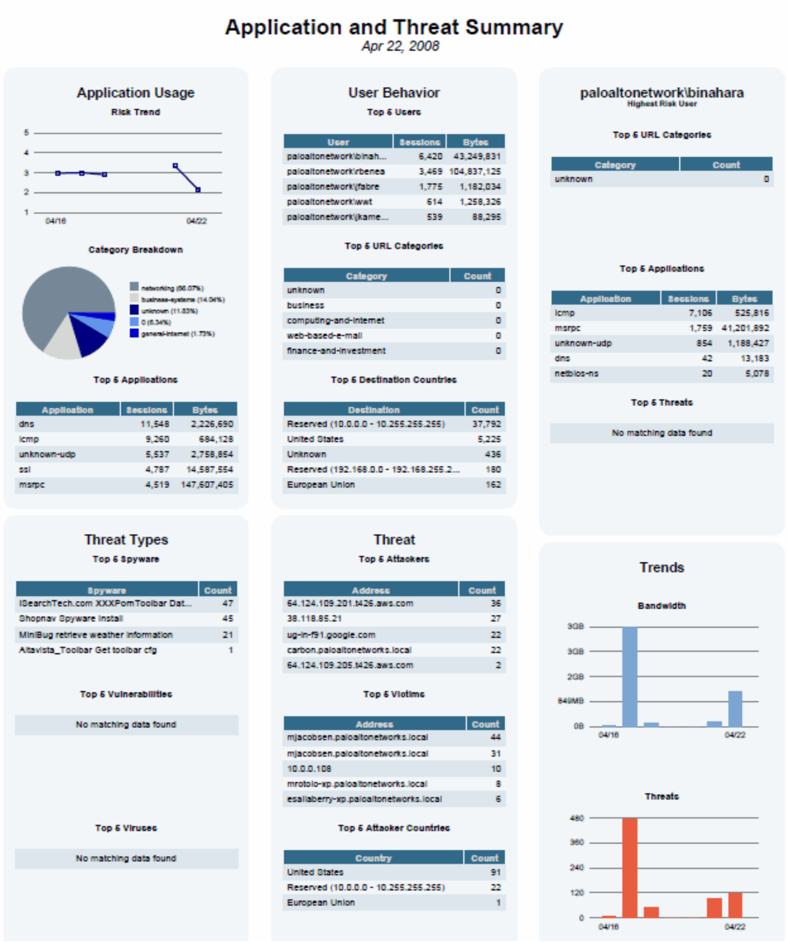
Table 184. Botnet Configuration Settings (Continued)

Field	Description
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**—The report includes traffic that involves up to the specified number of application sessions per hour. • **Destinations Per Hour**—The report includes traffic that involves up to the specified number of application destinations per hour. • **Minimum Bytes**—The report includes traffic for which the application payload equals or exceeds the specified size. • **Maximum Bytes**—The report includes traffic for which the application payload is equal to or less than the specified size.
IRC	Select the check box to include traffic involving IRC servers.

Managing PDF Summary Reports

▶ *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.



Application and Threat Summary

Apr 22, 2008

Application Usage

Risk Trend

Category Breakdown

Top 5 Applications

Application	Sessions	Bytes
dns	11,548	2,226,690
icmp	9,260	684,128
unknown-udp	5,537	2,758,854
ssl	4,787	14,587,554
msrpc	4,519	147,607,405

Threat Types

Top 5 Spyware

Spyware	Count
ISearchTech.com XXXPornToolbar Dat...	47
Shopnav Spyware Install	45
MiniBug retrieve weather information	21
Altavista_Toolbar Get toolbar cfg	1

Top 5 Vulnerabilities

No matching data found

Top 5 Viruses

No matching data found

User Behavior

Top 5 Users

User	Sessions	Bytes
paloaltonetwork\binah...	6,420	43,249,831
paloaltonetwork\rbenea	3,469	104,837,125
paloaltonetwork\jfabre	1,775	1,182,034
paloaltonetwork\wwt	614	1,258,326
paloaltonetwork\jkame...	539	88,295

Top 5 URL Categories

Category	Count
unknown	0
business	0
computing-and-internet	0
web-based-e-mail	0
finance-and-investment	0

Top 5 Destination Countries

Destination	Count
Reserved (10.0.0.0 - 10.255.255.255)	37,792
United States	5,225
Unknown	436
Reserved (192.168.0.0 - 192.168.255.2...	180
European Union	162

Threat

Top 5 Attackers

Address	Count
64.124.109.201.t426.aws.com	36
38.118.85.21	27
ug-in-f91.google.com	22
carbon.paloaltonetworks.local	22
64.124.109.205.t426.aws.com	2

Top 5 Victims

Address	Count
mjacobsen.paloaltonetworks.local	44
mjacobsen.paloaltonetworks.local	31
10.0.0.108	10
mrotolo-xp.paloaltonetworks.local	8
esallaberry-xp.paloaltonetworks.local	6

Top 5 Attacker Countries

Country	Count
United States	91
Reserved (10.0.0.0 - 10.255.255.255)	22
European Union	1

paloaltonetwork\binahara

Highest Risk User

Top 5 URL Categories

Category	Count
unknown	0

Top 5 Applications

Application	Sessions	Bytes
icmp	7,106	525,816
msrpc	1,759	41,201,892
unknown-udp	854	1,188,427
dns	42	13,183
netbios-ns	20	5,078

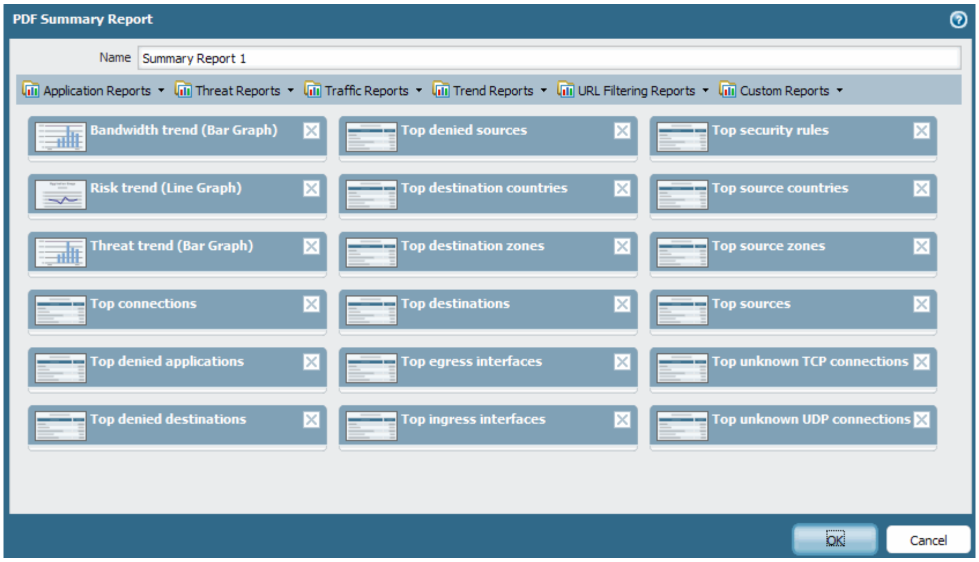
Top 5 Threats

No matching data found

Trends

Figure 13. PDF Summary Report

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



Name: Summary Report 1

Bandwidth trend (Bar Graph)
Top denied sources
Top security rules
Risk trend (Line Graph)
Top destination countries
Top source countries
Threat trend (Bar Graph)
Top destination zones
Top source zones
Top connections
Top destinations
Top sources
Top denied applications
Top egress interfaces
Top unknown TCP connections
Top denied destinations
Top ingress interfaces
Top unknown UDP connections

Figure 14. Managing PDF Reports

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

- To remove an element from the report, click the ⊟ icon in the upper-right corner of the element's icon box or remove the check box from the item in the appropriate drop-down list box near the top of the page.
- Select additional elements by choosing from the drop-down list boxes near the top of the page.
- Drag and drop an element's icon box to move it to another area of the report.

A maximum of 18 report elements is permitted. You may need to delete existing elements to add additional ones.

Click **Save**, enter a name for the report, as prompted, and click **OK**.

To display PDF reports, choose **PDF Summary Report**, and select a report type from the drop-down list at the bottom of the page to display the generated reports of that type. Click an underlined report link to open or save the report.

Managing User/Group Activity Reports

▶ *Monitor > PDF Reports > User Activity Report*

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

Table 185. User/Group Activity Report Settings

Field	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. On Panorama, you must have set up a master device for each device group in order to retrieve user group information for generating the report.
	For Group Activity Report: Select Group and enter the Group Name. On Panorama, you cannot generate Group Activity reports because Panorama does not have the information for mapping user(s) to group(s).
Time Period	Select the time frame for the report from the drop-down list.
Include Detailed Browsing	Select this option only if you wish to include detailed URL logs in the report. *The detailed browsing information can include a large volume of logs (thousands of logs) for the selected user or user group and can make the report 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, see “Scheduling Reports for Email Delivery”.

Managing Report Groups

▶ *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.

Table 186. Report Group Settings

Field	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 the check box to include a title page in the report.
Title	Enter the name that will appear as the report title.
Report selection	Select reports from the left column and click **Add** to move each report to the report group on the right. You can select Predefined, Custom, PDF Summary, and Log View report types. The **Log View** report is a report type that is automatically created each time you create a custom report and uses the same name as the custom report. This report will show the logs that were used to build the contents of the custom report. To include the log view data, when creating a report group, you add your custom report under the **Custom Reports** list and then add the log view report by selecting the matching report name from the **Log View** list. When you receive the report, you will see your custom report data followed by the log data that was used to create the custom report.

To use the report group, refer to “Scheduling Reports for Email Delivery”.

Scheduling Reports for Email Delivery

▶ *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 "Managing Report Groups" and "Configuring Email Notification Settings".

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

Table 187. Email Scheduler Settings

Field	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.
Report Group	Select the report group (refer to "Managing Report Groups").
Recurrence	Select the frequency at which to generate and send the report.
Email Profile	Select the profile that defines the email settings. Refer to "Configuring Email Notification Settings" for information on defining email profiles.
Override Recipient email(s)	Enter an optional email address to use instead of the recipient specified in the email profile.

Viewing 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 the reports, click the report names on the right side of the page (Custom Reports, Application Reports, Traffic Reports, Threat Reports, URL Filtering Reports, and PDF Summary Reports).

By default, all reports are displayed for the previous calendar day. To view reports for any of the previous days, select a report generation date from the **Select** drop-down list at the bottom of the page.

The reports are listed in sections. You can view the information in each report for the selected time period. To export the log in CSV format, click **Export to CSV**. To open the log information in PDF format, click **Export to PDF**. The PDF file opens in a new window. Click the icons at the top of the window to print or save the file.

Generating Custom Reports

▶ *Monitor > Manage Custom Reports*

You can create custom reports that are optionally based on existing report templates. The reports can be run on demand or scheduled to run each night. To view previously defined reports, choose **Reports** on the side menu.

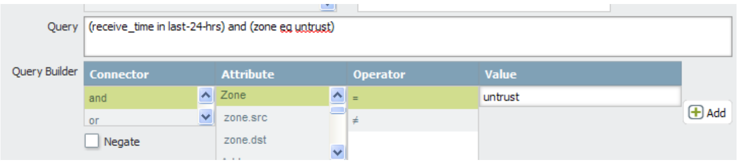
Click **Add** to create a new custom report. To base a report on an existing template, click **Load Template** and choose the template.

Specify the following settings to define the report.

Table 188. Custom Report Settings

Field	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.
Database	Choose the database to use as the data source for the report.
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.
Scheduled	Select the check box to run the report each night. The report then becomes available by choosing **Reports** on the side menu.
Columns	Choose the columns to include in the custom report from the **Available Column** list and use the plus icon ⊞ to move them to the **Selected Columns** list. Use the up and down arrows to reorder the selected columns, and use the minus icon ⊟ to remove previously selected columns.

Table 188. Custom Report Settings (Continued)

Field	Description
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) to precede the expression you are adding. • **Negate**—Select the check box 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. • **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 example, the following figure (based on the Traffic Log database) shows a query that matches if the traffic log entry was received in the past 24 hours and is from the "untrust" zone.  Query (receive_time in last-24-hrs) and (zone eq untrust) Value untrust Query Builder Connector Attribute Operator Value and or Negate Zone zone.src zone.dst = ≠ Add

For more information, see Generate Custom Reports.

Taking Packet Captures

▶ *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 have collected 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"*

What do you want to know?	See
Where do I download a packet capture?	▶ *"Packet Capture Overview"*
Do you want more? Can't find what you're looking for?	▶ ***How do I turn on extended packet capture for security profiles? See "Defining Content-ID Settings".*** ▶ ***How do I use packet captures to write custom application signatures? See Doc-2015. Note that this example uses a third-party app, but you can use the firewall to capture the required packets.*** ▶ ***How do I prevent a firewall admin from viewing packet captures? See defining** *Web Interface Administrator Access*.* ▶ ***For an example, see** *Take Packet Captures*.*

Packet Capture Overview

▶ *Monitor > Packet Capture*

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

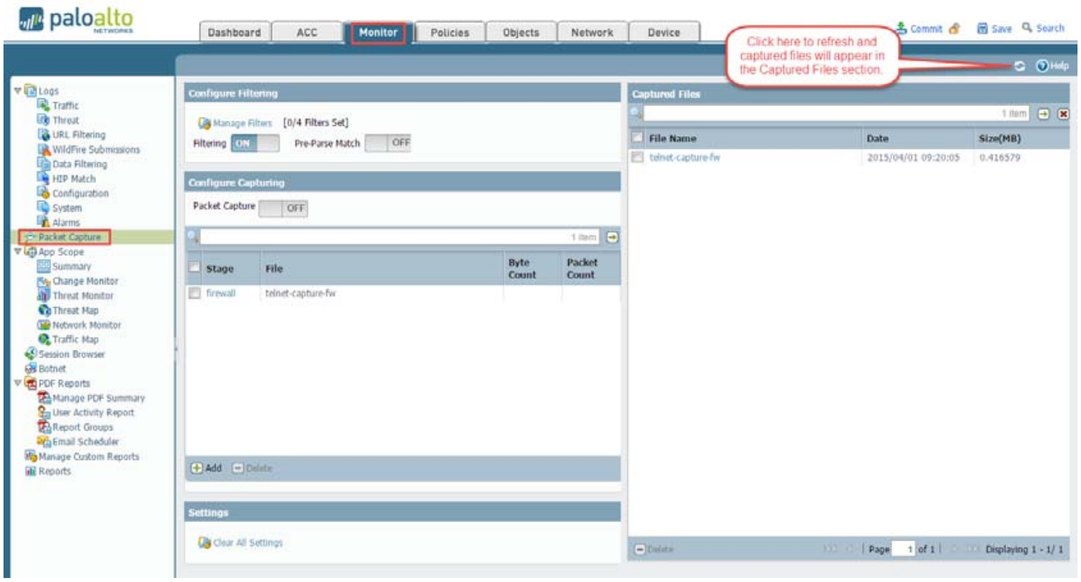
- Custom Packet Capture—Capture packets for all traffic or traffic based on filters that you define. For example, you can configure the firewall to capture only packets to and from a specific source and destination IP address or port. These packet captures are used to troubleshoot network traffic related issues or to gather application attributes to write custom application signatures. You configure this type of packet capture in **Monitor > Packet Capture**. You define the file name based on the stage (Drop, Firewall, Receive Transmit) and after the pcap is complete, you download the pcap in the Captures 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 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 the pcaps, select **Monitor > Threat**, and you will see the pcap download icon ⬇ in the second column of the threat log.

Building Blocks for a Custom Packet Capture

▶ *Monitor > 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.



Click here to refresh and captured files will appear in the Captured Files section.

Configure Filtering

Manage Filters [0/4 Filters Set]

Filtering ON Pre-Parse Match OFF

Configure Capturing

Packet Capture OFF

1 item

Stage	File	Byte Count	Packet Count
firewall	telnet-capture-fw		

Settings

Captured Files

1 item

File Name	Date	Size(MB)
telnet-capture-fw	2015/04/01 09:20:05	0.416579

Table 189. Building Blocks of a Custom Packet Capture

Field	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. • **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 the check box 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.

Table 189. Building Blocks of a Custom Packet Capture

Field	Configured In	Description
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	• **Packet Capture**—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. • **File**—Specify the capture file name. The file name should begin with a letter and can include letters, digits, periods, underscores, or hyphens. • **Byte Count**—Specify the maximum number of bytes, after which capturing stops. • **Packet Count**—Specify the maximum number of packets, after which capturing stops.

Table 189. Building Blocks of a Custom Packet Capture

Field	Configured In	Description
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, click the check box to the left of the file and then click **Delete** at the bottom of the window. • **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 the refresh icon 🔄 located above the Captured Files section before any new pcap files will appear in this list.
Clear All Settings	Settings	Click **Clear All Settings** to turn off packet capture and to clear all packet capture settings. Note that 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

▶ *Monitor > 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 **Monitor > Security Profiles** and then modify the desired profile as described in the following table:

Security Profile	Packet Capture Option
Antivirus	Select a custom antivirus profile and, in the **Antivirus** tab, select the **Packet Capture** check box.
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**.

Note: *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 (and 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 Policies Overview”.

Each time the firewall detects a threat when packet capture is enabled on the security profile, you can click the Packet Capture icon (⬇) located in the second column of the log to view or export the packet capture.

Chapter 7

Configuring the Firewall for User Identification

Configuring the Firewall for User Identification

▶ *Device > User Identification*

The User Identification (User-ID™) service is a Palo Alto Networks® next-generation firewall feature that allows you to create policies and perform reporting based on users and groups rather than individual IP addresses. If you are configuring a firewall with multiple virtual systems, you must create a separate User-ID configuration for each virtual system; user mapping information is not shared between virtual systems. Select the virtual system you want to configure for User-ID from the **Location** drop-down at the top of the User Identification page.

After selecting a virtual system (if applicable), use the settings on this page to configure the user identification settings.

- "User Mapping Tab"
- "User-ID Agents Tab"
- "Terminal Services Agents Tab"
- "Group Mapping Tab"
- "Captive Portal Settings Tab"

User Mapping Tab

Use the **User Mapping** tab to configure a firewall to retrieve IP address-to-username mapping data directly from domain servers. This feature does not require the installation of a User-ID agent on the domain servers. The firewall can also be configured to redistribute the user mapping information to other firewalls.

Table 190. User Mapping Settings

Field	Description
Palo Alto Networks User ID Agent Setup	
	This section of the screen shows the settings the firewall will use to perform IP address to user mapping. To configure the settings, click the Edit ⚙ icon to open the setup dialog, which contains the following tabs: • "WMI Authentication tab" • "Server Monitor tab" • "Client Probing tab" • "Cache tab" • "NTLM tab" • "Redistribution tab" • "Syslog Filters tab"
WMI Authentication tab	Use this subtab to set the domain credentials for the account the firewall will use to access Windows resources. This is required for monitoring Exchange servers and domain controllers as well as for WMI probing. **User Name**—Specify the account that has permissions to perform WMI queries on client computers and server monitoring. Enter the user name using the domain\username syntax. **Password/Confirm Password**—Specify the account password.

Table 190. User Mapping Settings (Continued)

Field	Description
Server Monitor tab	**Enable Security Log**—Select the check box to enable security log monitoring on Windows servers. Security logs will be queried to locate IP address to username mapping information on the servers specified in the **Server Monitoring** list. **Server Log Monitor Frequency (sec)**—Specify the frequency in seconds at which the firewall will query Windows servers for IP address to username mapping information (default is 2, range is 1-3600). This is the interval between when the firewall finishes processing the last query and when it starts the next query. **Enable Session**—Select the check box to enable monitoring of user sessions on the servers specified in the **Server Monitoring** list. Each time a user connects to a server, a session is created and this information can also be used to identify the user IP address. **Server Session Read Frequency (sec)**—Specify the frequency in seconds at which the firewall will query Windows server user sessions for IP address to username mapping information (default is 10, range is 1-3600). 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 IP address to username mapping information (default is 30, range is 1-3600). 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 service monitors. For details, see "Managing SSL/TLS Service Profiles". If you select **none**, the device uses its preconfigured, self-signed certificate. **WARNING:** *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*
Client Probing tab	**Enable Probing**—Select this check box to enable WMI/NetBIOS probing to each client PC identified by the user mapping process. Probing will help ensure that the same user is still logged into the client PC in order to provide accurate user to IP information. **Probe Interval (min)**—Specify the client PC probe interval (default is 20, range is 1-1440). 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 probe interval properly to allow time to probe each client that has been identified. Example, if you have 6,000 users and an interval of 10 minutes, it would require 10 WMI request a second from each client. **Note:** *If the probe request load is high, the observed delay between requests might significantly exceed the interval you specify.* **Note:** *For WMI polling to work effectively, the* ***User Mapping*** *profile must be configured with a domain administrator account, and each probed client PC must have a remote administration exception configured in the Windows firewall. For NetBIOS probing to work effectively, each probed client PC must allow port 139 in the Windows firewall and must also have file and printer sharing services enabled.*

Table 190. User Mapping Settings (Continued)

Field	Description
Cache tab	**Enable User Identification Timeout**—Select this check box to enable a timeout value for IP address-to-username mapping entries. When the timeout value is reached, the IP address-to-username mapping will be cleared and a new mapping will be collected. This will ensure that the firewall has the most current information as users roam around and obtain new IP addresses. **User Identification Timeout (min)**—Set the timeout value for IP address-to-username mapping entries (default 45 minutes; range 1-1440 minutes).
NTLM tab	**Enable NTLM authentication processing**—Select this check box to enable NT LAN Manager (NTLM) authentication processing. When Captive Portal rules have an action set to browser-challenge (see "Defining Captive Portal Policies") to capture user mapping information, an NTLM challenge transparently authenticates the client. With this option enabled, the firewall collects this information from the NTLM domain. When you configure the firewall to share its User-ID information with other PAN-OS firewalls (see "Redistribution tab"), it can serve NTLM requests coming from those firewalls, performing the function of the User-ID agent. **Note:** *If you use the Windows-based User-ID agent, NTLM responses go directly to the domain controller where you installed the agent.* **NTLM Domain**—Enter the NTLM domain name. **Admin User Name**—Enter the administrator account that has access to the NTLM domain. **WARNING:** *Do not include the domain in the* ***Admin User Name*** *field. Otherwise, the firewall will fail to join the domain.* **Password/Confirm Password**—Enter the password for the administrator account that has access to NTLM domain. **Note:** *You can only enable NTLM authentication processing on one virtual system (you select the virtual system from the* **Location** *drop-down at the top of the page).*
Redistribution tab	**Collector Name**—Specify the collector name if you want this firewall to act as a user mapping redistribution point for other firewalls on your network. The collector name and pre-shared key are used when configuring the User-ID agents on the firewalls that will pull the user mapping information. To enable a firewall to act as a redistribution point, you also need to enable the **User-ID** service in **Network > Network Profiles > Interface Mgmt**. **Pre-Shared Key/Confirm Pre-Shared Key**—Enter the pre-shared key that is used by other firewalls to establish a secure connection for user mapping transfers.

Table 190. User Mapping Settings (Continued)

Field	Description
Syslog Filters tab	Use this subtab to specify how the firewall should parse syslog messages to extract user mapping information (the IP address and the username) from the syslog messages it receives. To add a syslog filter, click **Add** and then complete the following fields. You can create separate filters for messages from different syslog senders. You must specify which filter to use when you add the sender to the list of monitored servers. In addition, before the syslog messages will be accepted on an interface, the syslog listener service must be enabled in management profile associated with the interface. **Syslog Parse Profile**—Enter a name for the parsing profile (up to 63 alpha-numeric characters). Palo Alto Networks provides several pre-defined syslog filters, which are delivered as Application content updates and are therefore updated dynamically as new filters are developed. The pre-defined filters are global to the firewall, whereas manually defined filters apply to a single virtual system only. **Description**—Enter a description for the profile (up to 255 alpha-numeric characters). **Type**—Specify the type of parsing to use to filter out the user mapping information. There are two supported types: **Regex Identifier** and **Field Identifier**. In order to create the filters, you must know the format of the authentication messages in the syslogs. The following field descriptions show examples for creating filters for a syslog messages that have the following format: `[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success User:domain\johndoe_4 Source:192.168.0.212` • **Regex Identifier**—With this type of parsing, you specify regular expressions to describe search patterns for identifying and extracting user mapping information from syslog messages. If you choose this option, you must specify the regex to use to match authentication events in the syslog message and to match the username and IP address fields within in the matching messages. • **Event Regex**—Use this field to specify the regex to identify successful authentication events within the syslog messages. For example, when matched against the example syslog message above, the following regex indicates that the firewall should match 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: `(authentication\ success){1}"`

Table 190. User Mapping Settings (Continued)

Field	Description
Syslog Filters tab (Continued)	– **Username Regex**—Enter the regex for identifying the beginning of the username in the authentication success messages. For example, the regex `User:([a-zA-Z0-9\\\._]+)` would match the string `User:johndoe_4` in the example message and extract acme\johndoe1 as the username. Use this field to specify the regex to identify the username field in the authentication success messages. – **Address Regex**—Use this field to specify the regex to identify the IP address field in the authentication success messages. For example, the following regular expression `Source:([0-9]{1,3}\.[0-9]){1,3}\.[0-9]{1,3}\.0-9]{1,3})` would match the string `Source:192.168.0.212` in the example message and extract and add 192.168.0.212 as the IP address in the username mapping that is created. • **Field Identifier** —With this type of parsing, you specify a sting to match the authentication event, and prefix and suffix strings to identify the user mapping information in the syslogs as follows: – **Event String**—Specify a string to identify the event log type from which to extract the user mapping information. For example, using the example syslog format shown above, you would enter the string `authentication success` to match on successful authentication events in the log. – **Username Prefix**—Enter the matching string for identifying the beginning of the username field within the authentication syslog message. For example, using the example syslog format shown above, you would enter the string `User:` to identify the beginning of the username. – **Username Delimiter**—Enter the delimiter used to mark the end of the username field within an authentication log message. For example, in the sample log message format, the username is followed by a space, so you would enter `\s` to indicate that the username field is delimited by a space. – **Address Prefix**—Specify a string to match to extract the IP address from the log message. For example, using the example syslog format shown above, you would enter the string `Source:` to identify the log field from which to extract the address. – **Address Delimiter**—Enter the matching string used to mark the end of the IP address field within the authentication success message. For example, in the sample log message format, the address is followed by a line break, so you would enter `\n` to indicate that the address field is delimited by a new line.

Table 190. User Mapping Settings (Continued)

Field	Description
Server Monitoring **Note:** *Keep in mind that for Active Directory (AD) events to be recorded in the security log, the AD domain must be configured to log successful account logon events.*	Use this section of the screen to define the Microsoft Exchange Servers, domain controllers, Novell eDirectory servers or syslog senders to monitor for logon events. For example, in an AD environment, the agent will monitor the security logs for Kerberos ticket grants or renewals, Exchange server access (if configured), and file and print service connections (for monitored servers). You can define entries for up to 50 syslog senders per virtual system and up to a total of 100 monitored servers, including syslog senders, Microsoft Active Directory, Microsoft Exchange, or Novell eDirectory servers. You can add other types of devices for discovery of user mapping information—such as wireless controllers, 802.1 devices, and/or Network Access Control (NAC) services—that the firewall can't monitor directly by setting them up as syslog senders. This is useful in environments where another device is already configured to authenticate end users. For this to work, you must also configure the firewall as a syslog listener (see "Defining Interface Management Profiles") and define how to filter the incoming syslog messages to extract the user mapping information (see "Syslog Filters tab"). To automatically discover Microsoft Active Directory domain controllers via DNS, click **Discover**. The firewall will discover domain controllers based on the domain name entered in the **Device > Setup > Management > General Settings** page, **Domain** field. You can then enable the servers you want to use to obtain user mapping information. **Note:** *The Discover feature works for domain controllers only; you cannot use it to auto-discover Exchange servers or eDirectory servers.* To manually define new servers to monitor or syslog senders to listen for, click **Add** and then complete the following fields: • **Name**—Enter a name for the server. • **Description**—Enter a description of the server to be monitored. • **Enabled**—Select the check box to enable this server for log monitoring. • **Type**—Select the type of server to monitor. Depending on the type, one or more of the following fields display: – **Network Address**—Enter the IP address or fully qualified domain name (FQDN) of the Exchange or Active Directory server to monitor. – **Server Profile**—Select the LDAP server profile to use to connect to the Novell eDirectory server. – **Connection Type**—Specifies whether the firewall agent will listen for syslog messages on the **UDP** port (514) or the **SSL** port (6514). If you select **SSL**, the **Syslog Service Profile** selected in the User ID Agent Setup settings (see "Server Monitor tab") determines the SSL/TLS versions that are allowed and the certificate that is used to establish a connection between the Syslog sender and the firewall. – **Filter**—Select which syslog filter to use to extract usernames and IP addresses from the syslog messages received from this server. – **Default Domain Name**—(Optional) Specify a domain name to prepend to the username if no domain name is present in the log entry. To finish adding the server, click **OK**. The firewall will attempt to connect to the server. Upon successfully connecting, the **Status** will display as **Connected**. If the firewall cannot connect, the **Status** will display an error condition, such as **Connection refused** or **Connection timeout**.

Table 190. User Mapping Settings (Continued)

Field	Description
Include/Exclude Networks	
	By default, if you do not specify subnetworks in this list, the User-ID agent will perform IP address to username mapping (discovery) for all the subnetworks of the servers in the **Server Monitoring** list. To limit discovery to specific subnetworks, click **Add** and specify a profile that comprises a **Name**, subnetwork IP address range (**Network Address**), **Discovery** option (**Include** or **Exclude**), and **Enabled** option (by which to enable or disable the profile). 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 do not 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. Note that if you add **Exclude** profiles without adding any **Include** profiles, the User-ID agent excludes all subnetworks, not just the ones you added. By default, the User-ID agent evaluates the profiles in the order you add them, from top-first to bottom-last. To change the evaluation order, click **Custom Include/Exclude Network Sequence**. In the dialog that opens, **Add**, **Delete**, **Move Up**, or **Move Down** the profiles to create a custom evaluation order. If you configure the firewall to distribute user mapping information to other firewalls, the discovery limits you specify in the **Include/Exclude Networks** list will apply to the distributed information. To apply the user mapping information to firewall traffic so that the information is available in logs, reports, and policies, you must **Enable User Identification** in each security zone (see "Defining Security Zones").

User-ID Agents Tab

Use the **User-ID Agents** tab to configure the firewall to interact with User Identification agents (User-ID agents) installed on directory servers on your network or with firewalls configured for agentless User-ID for the exchange of IP address to user mapping information.

A User-ID agent collects IP address to username mapping information from network resources and provides it to the firewall for use in security policies and logs.

User identification mapping requires that the firewall obtain the source IP address of the user before the IP address is translated with NAT. If multiple users appear to have the same source address, due to NAT or use of a proxy device, accurate user identification is not possible.

In environments where other network devices are already authenticating users, you can configure the authenticating service to forward event logs to the User-ID agent using syslog. The agent can then extract the authentication events from the syslogs and add them to the IP address to username mappings.

To add a new User-ID agent to the list of agents this firewall communicates with, click **Add** and complete the following fields.

Table 191. User-ID Agents Settings

Field	Description
Name	Enter a name to identify the User-ID 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 IP address of the Windows host on which the User-ID agent is installed.
Port	Enter the port number on which the User-ID agent is configured to listen for requests from the firewall. The default Windows User-ID agent service port number is 5007, however you can use any available port as long as the firewall and the User-ID agent use the same value. In addition, you can use different port numbers on different agents. **Note:** *Some earlier versions of the User-ID agent use 2010 as the default port.*
Collector Name	If this firewall is receiving user mapping information from another firewall that is configured for redistribution, specify the collector name configured on the firewall that will be collecting the user mapping data (this is displayed on the **Device > User Identification > User Mapping** tab).
Collector Pre-shared Key/Confirm Collector Pre-shared key	Enter the pre-shared key that will be used to allow SSL connectivity between the User-ID agent and the firewall that is acting as a distribution point for user mapping.
Use as LDAP Proxy	Select the check box to use this User-ID agent as a proxy for collecting group mapping information from a directory server and forwarding it to the firewall. To use this option, you must also configure group mapping on the firewall (see “Group Mapping Tab”). The firewall will push that configuration to the User-ID agent to enable it to collect the mapping information. This option is useful in deployments where the firewall cannot directly access the directory server. It is also useful in deployments that benefit from reducing the number of queries the directory server must process; multiple firewalls can receive the group mapping information from the cache on a single User-ID agent instead of each firewall directly querying the server.
Use for NTLM Authentication	Select the check box to use the configured User-ID agent to verify NTLM client authentication from the captive portal with the Active Directory domain.
Enabled	Select the check box to enable the firewall to communicate with this user identification agent. To finish adding the User-ID agent entry, click **OK**. The new User-ID agent is displayed on the list of agents. Verify that the icon in the Connected column is green, indicating that the firewall can successfully communicate with the agent. 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. If you want the firewall to communicate with agents in a specific order—for example, based on the proximity of the agents to the firewall or whether an agent is a backup or primary—click **Custom Agent Sequence** and then order the agents in the preferred order.

Terminal Services Agents Tab

Use the **Terminal Services Agents** tab to configure the firewall to interact with Terminal Services Agents (TS Agents) installed on your network. The TS Agent identifies individual users who are supported by the same terminal server and thus appear to have the same IP address. The TS Agent on a terminal server identifies individual users by allocating a specific port ranges to each individual user. When a port range is allocated for a particular user, the Terminal Services Agent notifies every connected firewall about the allocated port range so that policy can be enforced based on user and user groups.

To add a TS Agent to the firewall configuration, click **Add** and complete the following fields:

Table 192. Terminal Services Agents Settings

Field	Description
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 IP address of the terminal server on which the TS Agent is installed.
Port	Enter the port number on which the TS Agent service is configured to communicate with the firewall. The default port is 5009.
Alternative IP Addresses	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, click **Add** and then enter up to eight additional IP addresses.
Enabled	Select the check box to enable the firewall to communicate with this user identification agent. To finish adding the TS Agent entry, click **OK**. The new TS Agent is displayed on the list of agents. Verify that the icon in the Connected column is green, indicating that the firewall can successfully communicate with the agent. 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.

Group Mapping Tab

To define security policies based on user or group, the firewall must retrieve the list of groups and the corresponding list of members from your directory server. To enable this functionality, you must create an LDAP server profile (“Configuring LDAP Server Settings”) that instructs the firewall how to connect and authenticate to the LDAP directory server. The firewall supports a variety of LDAP directory servers, including Microsoft Active Directory (AD), Novell eDirectory, and Sun ONE Directory Server. After creating the server profile, use the **Group Mapping** tab to define how to search the directory for the user and group information. Use the **Custom Group** tab to create custom groups based on LDAP filters.

To add a group mapping configuration click **Add** and then enter a unique **Name** to identify the configuration. The name is case-sensitive and can be up to 31 characters, including letters, numbers, spaces, hyphens, and underscores. You must then complete the fields on the following subtabs:

- “Server Profile Subtab”
- “Group Include List Subtab”

- "Custom Group Subtab"

Server Profile Subtab

Use the Server Profile subtab to select an LDAP server profile to use for group mapping and specify how to search the directory for the specific objects that contain the user and group information

Table 193. Group Mapping Server Profile Settings

Field	Description
Server Profile	Select the LDAP server profile to use for group mapping on this firewall.
Update Interval	Specify the interval (seconds) after which the firewall will initiate a connection with the LDAP directory server to obtain any updates that have been made to the groups that are used in firewall policy (Range 60 to 86,400 seconds).
User Domain	By default, the **User Domain** field 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 device retrieves from the LDAP source. Your entry must be the NetBIOS name. **Note:** *This field only affects the usernames and group names retrieved from the LDAP source. For user authentication, to override the domain associated with a username, configure the **User Domain** and **Username Modifier** fields in the authentication profile that you assign to that user (see "Setting Up Authentication Profiles").*
Group Objects	• **Search Filter**—Specify an LDAP query that can be used to control which groups are retrieved and tracked. • **Object Clas**s—Specify the definition of a group. For example, the default is objectClass=group, which means that the system retrieves all objects in the directory that match the group filter and have objectClass=group. • **Group Name**—Enter the attribute that specifies the name of the group. For example in Active Directory, this attribute is "CN" (Common Name). • **Group Member**—Specify the attribute that contains the members of this group. For example in Active Directory, this attribute is "member."
User Objects	• **Search Filter**—Specify an LDAP query that can be used to control which users are retrieved and tracked. • **Object Clas**s—Specify the definition of the a user object. For example in Active Directory, the objectClass is "user." • **User Name**—Specify the attribute for user name. For example, in Active Directory, the default user name attribute is "samAccountName."

Table 193. Group Mapping Server Profile Settings (Continued)

Field	Description
Mail Domains	When the firewall receives a WildFire™ log for a malicious email, the email recipient information in the log is matched with the user mapping information that the User-ID agent collects. The log will contain a link to the user and when clicked, the ACC is displayed and filtered by the user. If the email is sent to a distribution list, the ACC is filtered by the members contained in the list. The email header and user mapping information will help you quickly track down and thwart threats that arrive via email by making it easier to identify the user(s) who received the email. • **Mail Attributes**—This field is automatically populated based on the LDAP server type (Sun/RFC, Active Directory, and Novell). • **Domain List**—Enter the list of email domains in your organization using a comma separated list up to 256 characters.
Enabled	To enable this server profile for group mapping, make sure this check box is selected.

Group Include List Subtab

Use the **Group Include List** subtab to limit the number of groups that appear when creating a security policy. Browse through the LDAP tree to find the groups you want to use in the policy.

To include a group, select it in the Available Groups list and click the Add ⊞ icon. The total number of groups you can add to a group mapping configuration (for both **Group Include List** subtab and **Custom Group** subtab combined) is 640 per virtual system.

To remove a group from the list, select it in the Included Groups list and click the Delete ⊟ icon.

Click **OK** to save the list of included groups.

Custom Group Subtab

Use the **Custom Group** subtab to 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 an LDAP-based service such as Active Directory (AD). 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 AD group domain name, the firewall uses the custom group in all references to that name (for example, in policies and logs).

The firewall does not validate LDAP filters.

After creating or cloning a custom group, you must perform a commit to make it available for use in policies and objects.

To create a custom group, click **Add**, enter a group **Name** (it must be unique in the group mapping configuration for the current firewall or virtual system), specify an **LDAP Filter** of up to 2,048 characters, and then click **OK**. The total number of groups you can add to a group mapping configuration (for both **Custom Group** subtab and **Group Include List** subtab combined) is 640 per virtual system.

To expedite LDAP searches and minimize the performance impact on the LDAP directory server, it is a best practice to use only indexed attributes in the filter.

To delete a custom group, select it and click **Delete**.

To make a copy of a custom group, select it, click **Clone**, edit the **Name** and **LDAP Filter** as desired, and then click **OK**.

Captive Portal Settings Tab

Use the **Captive Portal Settings** tab to configure captive portal authentication on the firewall. If the firewall receives a request from a zone that has the User-ID service enabled and the source IP address does not have any user data associated with it yet, it checks its Captive Portal policy for a match to determine whether to perform authentication. This is useful in environments where you have clients that are not logged in to your domain servers, such as Linux clients. This user mapping method is only triggered for web traffic (HTTP or HTTPS) that matches a security rule/policy, but that has not been mapped using a different method. For non-web-based traffic or traffic that does not match a captive portal policy, the firewall uses its IP-based security policies rather than the user-based policies.

To configure or edit the captive portal configuration, click the Edit ⚙ icon and complete the following fields:

Table 194. Captive Portal Settings

Field	Description
Enable Captive Portal	Select this check box to enable the captive portal option for user identification.
Idle Timer (min)	This is the user time to live (user TTL) setting for a captive portal session. This timer resets every time there is activity from a captive portal user. If the length of time the user is idle exceeds the idle timer, the captive portal user mapping will be removed and the user will have to log in again. (1-1440 minutes, default 15 minutes).
Timer (min)	This is the maximum TTL, which is the maximum amount of time that any captive portal session can remain mapped. After the expiration duration has elapsed, the mapping will be removed and users will have to re-authenticate even if the session is active. This timer is used to ensure prevent stale mappings and the value set here overrides the idle timeout. Therefore, as a best practice, set the expiration to a value that is higher than the idle timer (range 1 - 1440 minutes; default 60 minutes).
SSL/TLS Service Profile	To specify a certificate and the allowed protocols for securing redirect requests, select an SSL/TLS service profile. For details, see “Managing SSL/TLS Service Profiles”. If you select **None**, the firewall will use the local default certificate for SSL/TLS connections. 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 requests.
Authentication Profile	Select an authentication profile for authenticating users who are redirected to a web form for authentication. Note that even if you plan to use NTLM for authentication, you must configure either an authentication profile or a certificate profile to authenticate users if NTLM authentication fails or cannot be used because the client or browser does not support it.

Table 194. Captive Portal Settings (Continued)

Field	Description
Mode	Select a mode to define how web requests are captured for authentication: • **Transparent**—The firewall intercepts the browser traffic per the Captive Portal rule and impersonates the original destination URL, issuing an HTTP 401 to invoke authentication. However, because the firewall does not have the real certificate for the destination URL, the browser will display a certificate error to users attempting to access a secure site. Therefore you should only use this mode when absolutely necessary, such as in Layer 2 or virtual wire deployments. • **Redirect**—The firewall intercepts unknown HTTP or HTTPS sessions and redirects them to a Layer 3 interface on the firewall using an HTTP 302 redirect to perform authentication. This is the preferred mode because it provides a better end-user experience (no certificate errors). However, it does require additional Layer 3 configuration. Another benefit of the Redirect mode is that it provides for the use of 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 will not need to re-authenticate upon IP address change as long as the session stays open. In addition, if you plan to use NTLM authentication, you must use Redirect mode because the browser will only provide credentials to trusted sites. **Note:** *To use the captive portal in redirect mode, you must enable response pages on the interface management profile assigned to the Layer 3 interface to which you are redirecting the active portal. See "Defining Interface Management Profiles" and "Configure a Layer 3 Interface".*
Session Cookie (Redirect mode only)	• **Enable**—Select the check box to enable session cookies. • **Timeout**—If session cookies are enabled, this timer specifies the number of minutes the session cookie is valid. (range 60 - 10080 minutes; default 1440 minutes). • **Roaming**—Select the check box to retain the cookie if the IP address changes while the session is active (for example, if the client moves from a wired to wireless network). The user will only have to re-authenticate 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 you are redirecting requests.

Table 194. Captive Portal Settings (Continued)

Field	Description
Certificate Authentication	Select the **Certificate Profile** to use to authenticate captive portal users. When you use this type of authentication, the captive portal will prompt the browser to present a valid client certificate for authenticating the user. To use this method, you must provision client certificates on each user system and install the trusted CA certificate used to issue those certificates on the firewall. This is the only authentication method that enables transparent authentication for Mac OS and Linux clients.
NTLM Authentication	When captive portal is configured for NTLM authentication, the firewall uses an encrypted challenge-response mechanism to obtain the user's credentials from the browser. When configured properly, the browser will provide the credentials to the firewall transparently without prompting the user, but will display a prompt for credentials if necessary. If the browser cannot perform NTLM or if NTLM authentication fails, the firewall falls back to web form or client certificate authentication, depending on your Captive Portal configuration. By default, IE supports NTLM. Firefox and Chrome can be configured to use it. You cannot use NTLM to authenticate non-Windows clients. To configure NTLM for use with Windows-based User-ID agents, specify the following: • **Attempts**—Specify the number of attempts after which the NTLM authentication fails (Range 1-60; default 1). • **Timeout**—Specify the number of seconds after which the NTLM authentication times out (Range 1-60 seconds; default 2 seconds). • **Reversion Time**—Specify the time after which the firewall will again try to contact the first agent in the list of User-ID agents after the agent becomes unavailable (Range 60-3600 seconds; default 300 seconds). **Note:** *These options only apply to the User-ID agents installed on domain servers. When using the on-device User-ID agent, the firewall must be able to successfully resolve the DNS name of your Domain Controller in order for the firewall to join the domain. You can then enable NTLM authentication processing on the* ***User Mapping*** *tab and provide the credentials for the firewall to join the domain. For detailed step-by-step instructions, see the PAN-OS 7.0 Administrator's Guide.*

Chapter 8

Configuring IPSec Tunnels

This section describes basic virtual private network (VPN) technology and provides details on configuring and managing IP Security (IPSec) VPNs on Palo Alto Networks® firewalls.

Refer to the following topics:

- “Defining IKE Gateways”
- “Setting Up IPSec Tunnels”
- “Defining IKE Crypto Profiles”
- “Defining IPSec Crypto Profiles”
- “Defining GlobalProtect IPSec Crypto Profiles”

Defining IKE Gateways

▶ *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:

- “Managing IKE Gateways”
- “IKE Gateway General Tab”
- “IKE Gateway Advanced Options Tab”
- “Restart or Refresh an IKE Gateway”

Managing IKE Gateways

▶ *Network > Network Profiles > IKE Gateways*

The following table describes how to manage your IKE gateways.

Table 195 Manage IKE Gateways

Field	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**.

IKE Gateway General Tab

▶ *Network > Network Profiles > IKE Gateways*

The following table describes the beginning steps for how to configure an IKE gateway. IKE is Phase 1 of the IKE/IPSec VPN process. After performing these steps, see "IKE Gateway Advanced Options Tab".

Table 196. IKE Gateway General Settings

Field	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 if the peer also supports IKEv2, that is what they will use. Otherwise, the gateway falls back to IKEv1.
IPv4 / IPv6	Select the type of IP address the gateway uses.
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.
Peer IP Type	Select **Static** or **Dynamic** for the peer on the far end of the tunnel.
Peer IP Address	If **Static** is selected for **Peer IP Type**, specify the IP address of the peer on the remote end of the tunnel.
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 **Pre-Shared Key** is selected, 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.

Table 196. IKE Gateway General Settings (Continued)

Field	Description
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)**, I**P address**, **KEYID (binary format ID string in HEX)**, **User FQDN (email address)**. If no value is specified, the local IP address will be used as the Local Identification value.
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)**, **User FQDN (email address)**. If no value is specified, the peer’s IP address will be used as the **Peer Identification** value.

Table 196. IKE Gateway General Settings (Continued)

Field	Description
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 the Browse button to navigate to the location where the Certificate File is located. Click on the file and select Open, which populates the Certificate File field. • **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. – **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. **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. • **OCSP Responder**—Enter the OSCP 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.

Table 196. IKE Gateway General Settings (Continued)

Field	Description
HTTP Certificate Exchange	Click **HTTP Certificate Exchange** and enter the **Certificate URL** in order to use the Hash-and-URL method to notify the peer where to fetch the certificate. The Certificate URL is the URL of the remote server where you have stored your certificate. If the peer indicates that it too supports Hash and URL, 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. It will use 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**, **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**, **User FQDN (email address)**.
Peer ID Check	Select **Exact** or **Wildcard**. This setting applies to the Peer Identification that is being examined to validate the certificate. Suppose the Peer Identification was a Name equal to domain.com. If **Exact** is selected and the certificate in the IKE ID payload says the Name is mail.domain2.com, the IKE negotiation will fail. But if **Wildcard** is selected, any character in the Name string before the * must match, and any character after the * can differ.
Permit peer identification and certificate payload identification mismatch	Select this option 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 the local gateway sends to the peer gateway. See "Creating a Certificate Profile".
Enable strict validation of peer's extended key use	Select this option if you want to strictly control how the key can be used.

IKE Gateway Advanced Options Tab

▶ *Network > Network Profiles > IKE Gateways*

Use this tab to configure more advanced settings for an IKE gateway.

Table 197. IKE Gateway Advanced Options

Field	Description
Enable Passive Mode	Click to have the firewall only respond to IKE connections and never initiate them.

Table 197. IKE Gateway Advanced Options (Continued)

Field	Description
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 Subtab	
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 “Defining IKE Crypto Profiles”.
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 Subtab	
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 “Defining IKE Crypto Profiles”.
Strict Cookie Validation	Click to enable **Strict Cookie Validation** on the IKE gateway. • When **Strict Cookie Validation** is enabled, IKEv2 cookie validation is always enforced; the initiator must send an IKE_SA_INIT containing a cookie. • When **Strict Cookie Validation** is disabled (the default setting), 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.

Restart or Refresh an IKE Gateway

▶ *Network > IPSec Tunnels*

Open the **IPSec Tunnels** page, which indicates the status of tunnels. In the second **Status** column is a link to the IKE Info. Click the link for the gateway you want to restart or refresh. The IKE Info page opens. Click one of the entries in the list and click **Restart** or **Refresh**.

Table 198 IKE Gateway Restart or Refresh

Field	Description
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.

Setting Up IPSec Tunnels

▶ *Network > IPSec Tunnels*

Use the **IPSec Tunnels** page to establish and manage IPSec VPN tunnels between firewalls. This is the Phase 2 portion of the IKE/IPSec VPN setup.

To manage IPSec VPN tunnels, see the following:

- "Managing IPSec VPN Tunnels"

To configure an IPSec tunnel, use the following two tabs:

- "IPSec Tunnel General Tab"
- "IPSec Tunnel Proxy IDs Tab"

See the following when viewing IPSec tunnel status:

- "Viewing IPSec Tunnel Status on the Firewall"

To restart or refresh an IPSec tunnel, see the following:

- "Restart or Refresh an IPSec Tunnel"

Managing IPSec VPN Tunnels

▶ *Network > IPSec Tunnels*

The following table describes how to manage your IPSec VPN tunnels.

Table 199 Manage IPSec VPN Tunnels

Field	Description
Add	To create a new IPSec VPN tunnel, click **Add**. See "IPSec Tunnel General Tab" for instructions on configuring the new tunnel.
Delete	To delete a tunnel, select the tunnel and click **Delete**.
Enable	To enable a tunnel that has been disabled, select the tunnel and click **Enable**, which is the default setting for a tunnel.
Disable	To disable a tunnel, select the tunnel and click **Disable**.

IPSec Tunnel General Tab

Table 200. IPSec Tunnel General Tab Settings

Field	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 "Configure a Tunnel Interface".
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.

Table 200. IPSec Tunnel General Tab Settings (Continued)

Field	Description
Auto Key	If you choose **Auto Key**, specify the following: • **IKE Gateway**—Refer to "Defining 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 "Defining IPSec Crypto Profiles". • Click **Show Advanced Options** to access the remaining fields. • **Enable Replay Protection**—Select this option 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 option also copies the Explicit Congestion Notification (ECN) field. • **Tunnel Monitor**—Select this option to alert the device administrator of tunnel failures and to provide automatic failover to another interface. Note that 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 "Defining Monitor Profiles".
Manual Key	If you choose **Manual Key**, specify the following: • **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**, or **null** [no encryption]). • **Key/Confirm Key**—Enter and confirm an encryption key.

Table 200. IPSec Tunnel General Tab Settings (Continued)

Field	Description
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 this option to publish all routes from the satellite device 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 this option if you will use an external CA to manage certificates. Once you have your certificates generated, you will need to import them into the device and select the **Local Certificate** and the **Certificate Profile** to be used.

IPSec Tunnel Proxy IDs Tab

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.

Table 201. IPSec Tunnel Proxy IDs IPv4 and IPv6 Tab Settings

Field	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.

Table 201. IPSec Tunnel Proxy IDs IPv4 and IPv6 Tab Settings (Continued)

Field	Description
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.

Viewing 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.

Restart or Refresh an IPSec Tunnel

▶ *Network > IPSec Tunnels*

Open the **IPSec Tunnels** page, which indicates the status of tunnels. In the first **Status** column is a link to the Tunnel Info. Click on the link for the tunnel you want to restart or refresh. The **Tunnel Info** page for that tunnel opens. Click on one of entries in the list and then click **Restart** or **Refresh**.

Table 202 IPSec Tunnel Restart or Refresh

Field	Description
Restart	Restarts the selected tunnel. A restart will disrupt traffic going across the tunnel.
Refresh	Shows the current IPSec SA status.

Defining IKE Crypto Profiles

▶ *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 the **Move Up** or **Move Down** icon. 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.

Table 203. IKE Crypto Profile Settings

Field	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 the **Move Up** or **Move Down** icon 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 the **Move Up** or **Move Down** icon to change the order (top to bottom) to the following: **sha512**, **sha384**, **sha256**, **sha1**, **md5**.
Encryption	Select the check boxes for the desired Encapsulating Security Payload (ESP) authentication options. Click **Add** and select algorithms. For highest security, select an item and then click the **Move Up** or **Move Down** icon to change the order (top to bottom) to the following: **aes-256-cbc**, **aes-192-cbc**, **aes-128-cbc**, **3des**.
Key Lifetime	Select units and enter the length of time that the negotiated IKE Phase 1 key will be effective. Default: 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 reauthentication. A value of 0 disables the re-authentication feature.

Defining IPSec Crypto Profiles

▶ *Network > Network Profiles > IPSec Crypto*

Use the **IPSec Crypto Profiles** page to 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 "Defining GlobalProtect IPSec Crypto Profiles".

Table 204. IPSec Crypto Profile Settings

Field	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.
Encryption (**ESP** protocol only)	Click **Add** and select the desired encryption algorithms. For highest security, use the **Move Up** and **Move Down** buttons 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**, and **3des**. You can also select **null** (no encryption).
Authentication	Click **Add** and select the desired authentication algorithms. For highest security, use the **Move Up** and **Move Down** buttons 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).
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.

Defining GlobalProtect IPSec Crypto 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 device applies them, and can affect tunnel security and performance. To change the order, use the **Move Up** and **Move Down** buttons.

For VPN tunnels between GlobalProtect gateways and satellite devices (firewalls), see "Defining IPSec Crypto Profiles".

Table 205. GlobalProtect IPSec Crypto Profile Settings

Field	Description
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**.

Chapter 9
GlobalProtect Settings

Setting Up the GlobalProtect Portal

▶ ***Network > GlobalProtect > Portals***

Use this page to set up and manage a GlobalProtect™ portal configuration. The portal provides the management functions for the GlobalProtect infrastructure. Every client system that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the gateways. In addition, the portal controls the behavior and distribution of the GlobalProtect agent software to both Mac and Windows laptops. (On mobile devices, the GlobalProtect app is distributed through the Apple App Store for iOS devices or through Google Play for Android devices.)

To add a portal configuration, click **Add** to open the GlobalProtect Portal dialog. For detailed information on the fields on each tab of the dialog, see the following sections:

- "Portal Configuration Tab"
- "Client Configuration Tab"
- "Satellite Configuration Tab"

For detailed step-by-step instructions on setting up the portal, refer to "Configure a GlobalProtect Portal" in the *GlobalProtect Administrator's Guide*.

Portal Configuration Tab

Use the **Portal Configuration** tab to define the network settings to enable agents to connect to the portal and specify how the portal will authenticate end clients.

In addition, you can use this tab to optionally specify custom GlobalProtect portal login and help pages. For information on how to create and import these custom pages, refer to "Customize the Portal Login, Welcome, and Help Pages" in the *GlobalProtect Administrator's Guide*.

Table 206. GlobalProtect Portal Settings

Field	Description
Name	Enter 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 Multiple Virtual System Mode, the **Location** field does not appear in the GlobalProtect Portal dialog. After you save the portal, you cannot change its **Location**.
Network Settings	
Interface	Select the firewall interface that will be used as the ingress for remote clients/firewalls.
IP Address	Specify the IP address on which GlobalProtect portal web service will be running.
SSL/TLS Service Profile	To specify a certificate and the allowed protocols for securing the GlobalProtect portal, select a SSL/TLS service profile. For details, see “Managing SSL/TLS Service Profiles”. The Common Name (CN) and, if applicable, the Subject Alternative Name (SAN) fields of the certificate associated with the profile must exactly match the IP address or fully qualified domain name (FQDN) of the **Interface** you selected. As a best practice 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.
Authentication	
Authentication Profile	Choose an authentication profile to authenticate clients/satellites accessing the portal. If you are configuring LSVPN, you will not be able to save the configuration unless you select an authentication profile. Even if you plan to authenticate satellites using serial numbers, the portal requires an authentication profile to fall back to if it cannot locate or validate the serial number. Refer to “Setting Up Authentication Profiles”.
Authentication Message	Enter a message to help end users know what credentials they should use for logging in to the portal or use the default message. The message can be up to 50 characters in length.
Client Certificate	(Optional) If you plan to use mutual SSL authentication, select the certificate the client will present to the gateways. This client certificate will be distributed to all agents that successfully authenticated to the portal unless the corresponding client configuration for the agent contains a different client certificate. If you are using an internal CA to distribute certificates to clients, leave this field blank.
Certificate Profile	(Optional) Select the certificate profile to use to authenticate users on the portal. Only use this option if the end points will already have a client certificate pre-deployed using your internal public key infrastructure (PKI).
Appearance	

Table 206. GlobalProtect Portal Settings (Continued)

Field	Description
Disable login page	Select this option to disable access to the GlobalProtect portal login page from a web browser.
Custom Login Page	Choose an optional custom login page for user access to the portal.
Custom Help Page	Choose an optional custom help page to assist the user with GlobalProtect.

Client Configuration Tab

Use the **Client Configuration** tab to define the GlobalProtect client configuration settings that the portal will deploy to the agent/app upon successfully connecting and authenticating.

This tab also allows you to automatically deploy any **Trusted Root CA** certificates and intermediate certificates the end clients will need in order to establish HTTPS connections with the GlobalProtect gateways and/or the GlobalProtect Mobile Security Manager if these components are using server certificates that are not trusted by the end clients. Any certificates you add here will be pushed to the clients with the client configuration. To add a **Trusted Root CA** certificate, click **Add** and then select a certificate from the list or click **Import** to browse for and import the certificate onto the firewall.

If you have different classes of users requiring different configurations, you can create a separate client configuration for each. The portal will then use the username/group name and or OS of the client to determine which client configuration to deploy. As with security rule evaluation, the portal looks for a match starting from the top of the list. When it finds a match, it delivers the corresponding configuration to the agent/app. Therefore, if you have multiple client configurations it is important to order them so that more specific configurations (that is configurations for specific users or operating systems) are above more generic configurations. Use the **Move Up** and **Move Down** buttons to order the configurations. Click **Add** to open the Configs dialog and create a new client configuration. For detailed information on configuring the portal and creating a client configurations, refer to “Configure the GlobalProtect Portal” in the *GlobalProtect Administrator’s Guide*.

The Configs dialog contains five tabs, which are described in the following table:

- General tab
- User/User Group tab
- Gateways tab
- Agent tab
- Data Collection tab

Table 207. GlobalProtect Portal Client Configuration Settings

Field	Description
General Tab	
Name	Enter a name to identify this client configuration.

Table 207. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Use single sign-on	Select the check box to have GlobalProtect use the users' Windows login credentials to transparently connect and authenticate to the GlobalProtect portal and gateways. Users will not be required to enter a username and password in the agent Settings tab.
Config Refresh Interval (hours)	Specify the interval in hours at which to refresh the GlobalProtect agent configuration (default 24 hours; range 1-168 hours).
Authentication Modifier	• **None**—The portal always authenticates the agent using the specified authentication profile and/or certificate profile and sends the authentication credentials to the gateway. This is the default setting. • **Cookie authentication for config refresh**—Allow cookie-based agent authentication to the portal for refreshing a cached client configuration. • **Cookie Expire (days)**—This option displays only if you select **Cookie authentication for config refresh** from the **Authentication Modifier** field. Use it to specify the number of days that the agent can use the cookie to authenticate to the portal for a configuration refresh; a value of 0 (the default) indicates that the cookie never expires. • **Different password for external gateway**—Indicates that the portal and the gateway use different authentication credentials and prompts the user for gateway password after portal authentication succeeds. By default, the portal will send the same password the agent used to authenticate to the portal on to the gateway. • **Manual Gateway Only**—This option displays only if you select **Different password for external gateway** from the **Authentication Modifier** field. Select this check box if you want to be able to use different authentication mechanisms on different gateways that are configured as Manual gateways. For example, you might choose to use Active Directory credentials for an "always on" connection to one set of gateways, and use a stronger authentication mechanism, such as a two-factor OTP authentication on another set of gateways protecting more secure resources.
Connect Method	• **on-demand**—Select this option to allow users to establish a connection on demand. With this option, the user must explicitly initiate the connection. This function is primarily used for remote access connections. • **user-logon**—When this option is set, the GlobalProtect agent will automatically establish a connection after users log in to their computers. If you select **Use single sign-on**, the username and password used to log in to Windows is captured by the GlobalProtect agent and used to authenticate. • **pre-logon**—Allows the agent to authenticate and establish the VPN tunnel to the GlobalProtect gateway using a pre-installed machine certificate before the user has logged in to the machine. When using the pre-logon connect method, you can create GlobalProtect client configurations and security policies that specify pre-logon as the source user and enable access only to basic services, such as DHCP, DNS, Active Directory, and antivirus and operating system update services, to further speed up the login process for users. To use this feature, you must use your own public-key infrastructure (PKI) to issue and distribute certificates to your end-user systems. You must then import the root CA certificate used to issue the machine certificates onto the firewall (both the portal and the gateway) and then create a corresponding certificate profile.

Table 207. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Client Certificate	If you want to use mutual SSL authentication, select the certificate the client will present to the gateways. This client certificate will be distributed to all agents that match this client configuration. If there is also a client certificate specified on the **Portal Configuration** tab, this one will be used instead. If you are deploying unique certificates to your end points using an internal PKI, leave this field blank.
Mobile Security Manager	If you are using the GlobalProtect Mobile Security Manager for mobile device management, 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 device should use when connecting to the GlobalProtect Mobile Security Manager for enrollment. By default, the Mobile Security Manager listens on port 443 and it is a best practice to leave it set to this value so that mobile device users are not prompted for a client certificate during the enrollment process. (Default: 443; Possible values: 443, 7443, 8443)
Internal Host Detection	With this option, GlobalProtect does a reverse DNS lookup of the specified **Hostname** to the specified **IP Address**. If it does not match, GlobalProtect determines the end point is outside of the corporate network and establishes a tunnel with any of the available external gateways configured in the **Gateways** tab. If it matches, the agent determines that the end point is inside the network and connects to an internal gateway (if configured); it does not create a VPN connection to any external gateways in this case. Select the check box to enable internal host detection using DNS lookup. Specify the following: • **IP Address**—Enter an internal IP address for the internal host detection. • **Hostname**—Enter the hostname that resolves to the above IP address within the internal network.
User/User Group Tab	
	Specify the user or user group to and/or client operating system to which to apply the client configuration: • **User/User Group**—Click **Add** to select a specific user or user group to which this configuration will apply from the list (group mapping must be configured for the list of users and groups to display). You can also create configurations to be deployed to agents in **pre-logon** mode (that is, before the user has logged in to the system), or configurations to be applied to **any** user. • **OS**—To deploy configurations based on the specific operating system running on the end system, click **Add** in the OS section of the Window and then select the applicable operating systems (**Android**, **iOS**, **Mac**, or **Windows**). Or leave the value in this section set to **Any** for the configurations to be deployed based on user/group only.

Table 207. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Gateways Tab	
Cutoff Time	Specify the amount of time (in seconds) the agent will wait for gateways to respond before determining the best gateway to connect to. The agent will then attempt to connect to only those gateways that responded within the specified Cutoff Time. The default value is 5. A value of 0 indicates that there is no cutoff time; the agent will wait until the TCP timeout. (Range 0 to 10)
Internal Gateways	Specify the internal firewalls that the agent will authenticate and provide HIP reports to.
External Gateways	Specify the list of firewalls the agent should try to establish a tunnel with when not on the corporate network Click **Add** and then enter the following information for each external gateway: • **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) field in the gateway server certificate (for example, if you used a FQDN to generate the certificate, you must also enter the FQDN here). • **Priority**—Select a value (**Highest**, **High**, **Medium**, **Low**, **Lowest**, or **Manual only**) to help the agent determine which gateway to connect to. The agent will contact all of the gateways (except those with a priority of **Manual only**) and establish a tunnel with the firewall that provides the fastest response and the highest Priority value. • **Manual**—Select this check box if you want to allow users to manually connect to (or switch to) the gateway. The GlobalProtect agent will have the option to connect to any external gateway that is configured as **Manual** selection. When connecting to the new gateway, the existing tunnel will be disconnected and a new tunnel will be established. The manual gateways can also have different authentication mechanism than the primary gateway. If the client system is restarted, or if a rediscovery is performed, the GlobalProtect agent will connect to the primary gateway. This feature is useful if you have a group of users who need to temporarily connect to a specific gateway to access a secure segment of your network.
Agent Tab	The settings on this tab specify how end users interact with the GlobalProtect agents installed on their systems. You can define different agent settings for the different GlobalProtect client configurations you create.
Passcode/Confirm Passcode	Enter the passcode that end users will need to enter to override the agent. This field is only required if the Agent User Override field is set to with-passcode.

Table 207. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Agent User Override	Select an override option: • **disabled**—Prevents end users from disabling the GlobalProtect agent. • **with-comment**—Prompts the end user to enter a comment when disabling the GlobalProtect agent. • **with-passcode**—The option allows the user to enter a passcode to override the GlobalProtect agent. If you select this option, you must also enter a value in the **Passcode** and **Confirm Passcode** field. Users will have to enter this value in order to override the agent. • **with-ticket**—This option enables a challenge-response mechanism to authorize disabling GlobalProtect agent on the client side. When this option is selected, the user is prompted with a challenge when disabling GlobalProtect. The challenge is then communicated to the firewall administrator out-of-band, and the administrator can validate the challenge through the firewall management interface. The firewall produces a response that is read back to the user who can then disable GlobalProtect by entering the response when prompted by the GlobalProtect agent. When using this option, you must also enter the key for decrypting the ticket in the **Agent User Override Key** fields at the top-level of the **Client Configuration** tab.
Max Agent User Overrides	Specify the maximum number of times a user can disable GlobalProtect before a successful connection to a firewall is required. A value of 0 (the default) indicates that agent overrides are unlimited.
Agent User Override Timeout	Specify the maximum length of time (in minutes) that GlobalProtect will be disabled upon override; after the specified amount of time elapses, the agent will reconnect. A value of 0 (the default) indicates that the duration of the override is unlimited.
Agent Upgrade	Select one of the following options to specify how GlobalProtect agent software downloads/upgrades will occur: • **disabled**—Prevents users from upgrading the agent. • **manual**—Allow users to manually check for and initiate upgrades by selecting the agent Check Version option. • **prompt**—Prompt end users to upgrade whenever a new agent version is activated on the firewall. This is the default setting. • **transparent**—Automatically upgrade the agent software whenever a new version is available on the portal.
Welcome Page	Select a welcome page to display to end users upon successfully connecting to GlobalProtect. You can select the **factory-default** page or **Import** a custom page. By default this field is set to **None**.
Third Party VPN	Click **Add** to add a list of third-party remote access VPN clients that might be present on the end points. If configured, GlobalProtect will ignore those VPN clients and their route settings to ensure that it does not interfere or conflict with them.
Enable advanced view	Deselect this check box to restrict the user interface on the client side to the basic minimum view. By default, the advanced view setting is enabled.

Table 207. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Show GlobalProtect icon	Clear this check box to hide the GlobalProtect icon on the client system. When hidden, users cannot perform other tasks such as changing passwords, rediscovering the network, resubmitting host information, viewing troubleshooting information, or performing an on-demand connection. However, HIP notification messages, login prompts, and certificate dialogs will still display as necessary for interacting with the end user.
Allow user to change portal address	Clear this check box disable the **Portal** field on the **Settings** tab in the GlobalProtect agent. 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: (HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks®\GlobalProtect\PanSetup with key Portal) or the Mac plist (/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist with key Portal).
Enable "Do not display this welcome page again" check box	Clear this check box to force the Welcome Page to display each time a user initiates a connection. This prevents the user from dismissing important information such as terms and conditions that may be required by your organization to maintain compliance.
Allow user to save password	Clear this check box to prevent users from saving their passwords on the agent (that is, you want to force them to provide the password—either transparently via the client or by manually entering one—each time they connect).
Enable Rediscover Network option	Clear this check box to prevent users from performing a manual network rediscovery.
Enable Resubmit Host Profile option	Clear this check box to prevent users from manually triggering resubmission of the latest HIP.
Allow user to continue if portal server certificate is invalid	Clear this check box to prevent the agent from establishing a connection with the portal if the portal certificate is not valid.
Data Collection Tab	Use this subtab to define what data the agent will collect from the client in the HIP report:
Collect HIP Data	Clear this check box to prevent the agent from collecting and sending HIP data.
Max Wait Time	Specify how long the agent should search for the HIP data before submitting the information available (range 10-60 seconds; default 20 seconds).
Exclude Categories	Use this subtab to define any host information categories for which you do not want to collect HIP data. Select a **Category** to exclude from HIP collection. After selecting a category, optionally refine the exclusion by clicking **Add** and then selecting the particular **Vendor**. Click **Add** in the Product section of the dialog and then select the products from the vendor. Click **OK** to save settings.

Table 207. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Custom Checks	Use this subtab to define any custom host information that you want the agent to collect. For example, if you have any required applications that are not included in the Vendor and/or Product lists for creating HIP objects, create a custom check that will allow you to determine whether that application is installed (has a corresponding registry or plist key) or is running (has a corresponding running process): • **Windows**—Click **Add** to add a check for a particular registry key and/or key value. • **Mac**—Click **Add** to add a check for particular plist key or key value. • **Process List**—Click **Add** to specify the list of processes to be checked on the end user systems 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 List to the **Windows** tab or the **Mac** tab.

Satellite Configuration Tab

A satellite device is a Palo Alto Networks firewall—typically at a branch office—that acts as a GlobalProtect agent to enable it to establish VPN connectivity to a GlobalProtect gateway. Like a GlobalProtect agent, the satellite receives its initial configuration from the portal, which includes the certificates and VPN configuration routing information to enable it to connect to all configured gateways to establish VPN connectivity.

Before configuring the GlobalProtect satellite settings on the branch office firewall, you must first 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 configure the GlobalProtect satellite settings on the portal as described in the following table:

Table 208. GlobalProtect Portal Satellite Configuration Settings

Field	Description
General subtab	Click **Add** to display the subtabs, and specify the following on the **GlobalProtect Satellite > General** subtab: • **Name**—Enter a name to identify the GlobalProtect satellite device profile. • **Configuration Refresh Interval (hours)**—Specify how often satellite devices should check the portal for configuration updates (default 24 hours, range 1-48 hours).
Devices subtab	Click **Add** to manually add a satellite device using the device serial number. If you use this option, when the satellite device first connects to receive the authentication certificate and the initial configuration, no user login prompt is required. After the satellite device authenticates, the **Name** (host name) will be added automatically to the Portal.

Table 208. GlobalProtect Portal Satellite Configuration Settings (Continued)

Field	Description
Enrollment User/User Group subtab	The portal uses the **Enrollment User/User Group** settings and/or **Devices** serial numbers to match a satellite to a configuration. Specify the match criteria for the satellite configuration as follows: • To restrict this configuration to satellite devices with specific serial numbers, select the **Devices** tab, click **Add**, and enter serial number (you do not need to enter the satellite hostname; it will be automatically added when the satellite connects). Repeat this step for each satellite you want to receive this configuration. • Select the **Enrollment User/User Group** tab, click **Add**, and then select the user or group you want to receive this configuration. Satellites that do not match on serial number will be required to authenticate as a user specified here (either an individual user or group member). **Note:** *Note Before you can restrict the configuration to specific groups, you must enable Group Mapping.*
Gateways subtab	Click **Add** to enter the IP address or hostname of the gateway(s) satellites with this configuration can establish IPSec tunnels with. Enter the FQDN or IP address of the interface where the gateway is configured in the **Gateways** field (Optional) If you are adding two or more gateways to the configuration, the **Routing Priority** helps the satellite pick the preferred gateway. Enter a value in the range of 1-25, with lower numbers having the higher priority (that is, the gateway the satellite will connect to if all gateways are available). The satellite will multiply the routing priority by 10 to determine the routing metric. **Note:** *Routes published by the gateway are installed on the satellite as static routes. The metric for the static route is 10x the routing priority. If you have more than one gateway, make sure to also set the routing priority to ensure that routes advertised by backup gateways have higher metrics compared to 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 will also share its network and routing information with the gateways if the **Publish all static and connected routes to Gateway** (configured on the satellite in **Network > IPSec tunnels > Advanced** tab) option is selected. See "GlobalProtect Satellite" for more details.
Trusted Root CA	Click **Add** and then select the CA certificate used to issue the gateway server certificates. As a best practice, all of your gateways should use the same issuer. **Note:** *If the root CA certificate used to issue your gateway server certificates is not on the portal, you can* **Import** *it now.*
Issuing Certificate	Select the Root CA certificate that for the portal to use to issue certificates to satellites upon successfully authenticating them.
Validity Period (days)	Specify the issued GlobalProtect satellite certificate lifetime (default 7 days, range 7-365 days).

Table 208. GlobalProtect Portal Satellite Configuration Settings (Continued)

Field	Description
Certificate Renewal Period (days)	Specify the GlobalProtect satellite certificate renewal period (default 3 days, range 3-30 days). This will determines how often certificates should be renewed.
OCSP Responder	Select the OCSP responder for the satellites to use to verify the revocation status of certificates presented by the portal and gateways.

Setting Up the GlobalProtect Gateways

▶ *Network > GlobalProtect > Gateways*

Use this page to configure a GlobalProtect gateway. The gateway can be used to provide VPN connections for GlobalProtect agents/apps or GlobalProtect satellite devices.

To add a gateway configuration, click **Add** to open the GlobalProtect Portal dialog. For detailed information on the fields on each tab of the dialog, see the following sections:

- "General Tab"
- "Client Configuration Tab"
- "Satellite Configuration Tab"

For detailed step-by-step instructions on setting up a gateway, refer to "Configure a GlobalProtect Gateway" in the *GlobalProtect Administrator's Guide*.

General Tab

Use the **General** tab to define the gateway interface to which agents/apps will connect and specify how the gateway will authenticate end clients.

Table 209. GlobalProtect Gateway General Settings

Field	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 Multiple Virtual System Mode, the **Location** field does not appear in the GlobalProtect Gateway dialog. After you save the gateway, you cannot change its **Location**.
Network Settings	
Interface	Select the firewall interface that will be used as the ingress for remote agents/satellites.
IP Address	Specify the IP address for gateway access.
SSL/TLS Service Profile	To specify a certificate and the allowed protocols for securing the GlobalProtect gateway, select a SSL/TLS service profile. For details, see "Managing SSL/TLS Service Profiles".

Table 209. GlobalProtect Gateway General Settings (Continued)

Field	Description
Authentication	
Authentication Profile	Choose an authentication profile or sequence to authenticate access to the gateway. Refer to "Setting Up Authentication Profiles".
Authentication Message	Enter a message to help end users know what credentials they should use for logging in to this gateway or use the default message. The message can be up to 50 characters in length.
Certificate Profile	Choose the certificate profile for client authentication.

Client Configuration Tab

Use the Client Configuration tab to configure the tunnel settings to enable agents/apps to establish VPN tunnels with the gateway. In addition, use this tab to define HIP notification messages to display to end users upon matching/not matching a HIP profile attached to a security policy.

This tab contains the three subtabs, which are described in the following table:

- "Tunnel Settings Subtab"
- "Network Settings Subtab"
- "Network Services Subtab"
- "HIP Notification Subtab"

Tunnel Settings Subtab

Use this subtab to configure the tunnel parameters and enable tunneling.

The tunnel parameters are required if you are setting up an external gateway. If you are configuring an internal gateway, they are optional.

Table 210. GlobalProtect Gateway Client Tunnel Mode Configuration Settings

Field	Description
Tunnel Mode	Select the check box to enable tunnel mode and specify the following settings: • **Tunnel Interface**—Choose the tunnel interface for access to the gateway. • **Max User**—Specify the maximum number of users that can access the gateway at the same time for authentication, HIP updates, and GlobalProtect agent updates. If the maximum number of users is reached, subsequent users are denied access with an error message indicating that the maximum number of users has been reached. By default, there is no limit set (range=1-1024 users). • **Enable IPSec**—Select the check box to enable IPSec mode for client traffic, making IPSec the primary and SSL-VPN the fall back method. • **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 “Defining GlobalProtect IPSec Crypto Profiles”. • **Enable X-Auth Support**—Select the check box 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 the **X-Auth Support** check box enables 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 user name 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** check box.
Timeout Configuration	Specify the following timeout settings: • **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 number of minutes at which a client is logged out of GlobalProtect if the GlobalProtect app has not routed traffic through the VPN tunnel in the given amount of time.

Network Settings Subtab

The Network Settings options are available only if you have enabled Tunnel Mode and defined a Tunnel Interface on the Tunnel Settings tab.

The network settings defined here will be assigned to the virtual network adapter on the client system when an agent establishes a tunnel with the gateway.

Table 211. GlobalProtect Gateway Client Network Configuration Settings

Field	Description
User/User Group subtab	Specify the user or user group to and/or client operating system to which to apply the client configuration.
User/User Group	Click **Add** to select a specific user or user group to which this configuration will apply from the list (group mapping must be configured for the list of users and groups to display). You can also create configurations to be deployed to agents in **pre-logon** mode (that is, before the user has logged in to the system) or configurations to be applied to **any** user.
OS	To deploy configurations based on the specific operating system running on the end system, click **Add** in the OS section of the Window and then select the applicable operating systems (**Android**, **iOS**, **Mac**, or **Windows**). Or leave the value in this section set to **Any** for the configurations to be deployed based on user/group only.
Network Settings subtab	
Retrieve Framed-IP-Address attribute from authentication server	Select the check box to enable the GlobalProtect gateway to assign fixed IP addresses using an external authentication server. When enabled, the GlobalProtect gateway allocates the IP address to connecting devices using the Framed-IP-Address attribute from the authentication server.
Authentication Server IP Pool	This section is only available if the **Retrieve Framed-IP-Address attribute from authentication server** option is enabled. Click **Add** to specify Authentication Server IP pool settings. Use this section to create 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. **Note:** *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. Configuring multiple ranges from different subnets will allow the system to offer clients an IP address that does not conflict with other interfaces on the client.* The servers/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.

Table 211. GlobalProtect Gateway Client Network Configuration Settings (Continued)

Field	Description
IP Pool	Click **Add** to specify IP pool settings. Use this section to create a range of IP addresses to assign to remote users. When the tunnel is established, an interface is created on the remote user's computer with an address in this range. **Note:** *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 will allow the system to offer clients an IP address that does not conflict with other interfaces on the client.* The servers/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.
No direct access to local network	Select the check box to disable split tunneling including direct access to local networks on Windows and Mac OS systems. This prevents users 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.
Access Route	Click **Add** to specify access route options. Use this section to add routes that will be pushed to the remote user's computer and therefore determine what the user's computer will send through the VPN connection. For example, you can set up split tunneling to allow remote users to access the Internet without going through the VPN tunnel. If no route is added, then 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 the user's computer and then gaining access to the internal network (with the user's computer acting as bridge).

Network Services Subtab

The Network Services options are available only if you have enabled Tunnel Mode and defined a Tunnel Interface on the Tunnel Settings tab.

On this tab, you can configure DNS settings that will be assigned to the virtual network adapter on the client system when an agent establishes a tunnel with the gateway.

Table 212. GlobalProtect Gateway Client Network Services Configuration Settings

Field	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 agents' configuration. With this setting all client network configuration, 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 the link to see the server settings that are currently assigned to the client interfaces.

Table 212. GlobalProtect Gateway Client Network Services Configuration Settings

Field	Description
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 clients.
DNS Suffix	Click **Add** to enter a suffix that the client 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 Suffixes	Select this check box to inherit the DNS suffixes from the inheritance source.

HIP Notification Subtab

Use this subtab to define the notification messages end users will see when a security rule with a host information profile (HIP) is enforced.

This step only applies if you have created host information profiles and added them to your security policies.

Table 213. GlobalProtect Gateway Client HIP Notification Configuration Settings

Field	Description
HIP Notification	Click **Add** to specify notification options. Select **Enable** to enable the **Match Message** and/or **Not Match Message**. Choose a notification option from the **Show Notification As** section and choose the radio button for a **System Tray Balloon** or **Pop Up Message**, and then specify a message to match or not match. Use these settings to notify the end user about the state of the machine, for example, to provide 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. **Note:** *The HIP notification messages can be formatted in rich HTML, which can include links to external web sites and resources. Use the link icon* 🔗 *in the rich text settings toolbar to add links.*

Satellite Configuration Tab

A satellite device is a Palo Alto Networks firewall—typically at a branch office—that acts as a GlobalProtect agent to enable it to establish VPN connectivity to a GlobalProtect gateway. Use the **Satellite Configuration** tab to define the gateway tunnel and network settings to enable the satellite devices to establish VPN connections with it. You can also use this tab to control the routes advertised by the satellites.

This tab contains the three subtabs, which are described in the following table:

- Tunnel Settings subtab
- Network Settings subtab
- Route Filter subtab

Table 214. GlobalProtect Gateway Satellite Configuration Settings

Field	Description
Tunnel Settings subtab	
Tunnel Configuration	Select the **Tunnel Configuration** check box and select an existing **Tunnel Interface**, or click **New Tunnel Interface**. See "Configure a Tunnel Interface"for more information. **Replay attack detection—**Protect against replay attacks. **Copy TOS**—Copy the (Type of Service) ToS header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original ToS information. **Configuration refresh interval (hours)**—Specify how often satellite devices should check the portal for configuration updates (default 2 hours; range 1-48 hours).
Tunnel Monitoring	Select the **Tunnel Monitoring** check box to enable the satellite devices to monitor gateway tunnel connections, allowing them to failover to a backup gateway if the connection fails. **Destination IP**—Specify an IP 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.
Crypto Profiles	Select an **IPSec Crypto Profile**, or create a new profile. This will determine 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 can typically use the default profile, which uses ESP protocol, DH group2, AES 128 CVC encryption, and SHA-1 authentication. See "Defining IPSec Crypto Profiles"for more details.
Network Settings subtab	
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.
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 check box to send the DNS suffix to the satellite devices to use locally when an unqualified hostname is entered that it cannot resolve.

Table 214. GlobalProtect Gateway Satellite Configuration Settings (Continued)

Field	Description
IP Pool	Click **Add** to specify IP pool settings. Use this section to create a range of IP addresses to assign to the tunnel interface on satellite devices upon establishment of the VPN tunnel. **Note:** *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 device.* The servers/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 may 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 the 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 will route traffic that is not destined for a specified access route using its own routing table. For example, you may choose to only tunnel traffic destined for your corporate network, and use the local satellite to safely enable Internet access. • If you want to enable routing between satellites, enter the summary route for the network protected by each satellite.
Route Filter subtab	Select the **Accept published routes** check box to accept routes advertised by the satellite into the gateway's routing table. If you do not select this option, the gateway will not accept any routes advertised by the satellites. If you want to be more restrictive on accepting the routes advertised by the satellites, click **Add** in the Permitted subnets section to define the subnets for which the gateway should accept routes; subnets advertised by the satellites that are not part of the list will be 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 will result in the gateway accepting the routes from the satellite only if it is in the 192.168.0.0/16 subnet.

Setting Up Gateway Access to a Mobile Security Manager

▶ *Network > GlobalProtect > MDM*

If you are using a Mobile Security Manager to manage end user mobile devices 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 devices. Use this page to enable the gateway to access the Mobile Security Manager.

To add information for a Mobile Security Manager, click **Add**. The following table provides information on what to enter in the fields on the GlobalProtect MDM dialog. For more detailed information on setting up the GlobalProtect Mobile Security Manager service, refer to "Set Up the GlobalProtect Mobile Device Manager" in the *GlobalProtect Administrator's Guide*. For detailed step-by-step instructions for setting up the gateway to retrieve the HIP reports on the GlobalProtect Mobile Security Manager, refer to "Enable Gateway Access to the GlobalProtect Mobile Security Manager."

Table 215. GlobalProtect MDM Settings

Field	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.
Location	For a firewall that is in Multiple Virtual System Mode, the **Location** is the virtual system (vsys) where the Mobile Security Manager is available. For a firewall that is not in Multiple Virtual System Mode, the **Location** 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 will connect to retrieve HIP reports. Ensure that you have a service route to this interface.
Connection Port	The port the Mobile Security Manager will listen on for HIP report requests. The default port is 5008, which is the port that the GlobalProtect Mobile Security Manager listens on. 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 establishing an HTTPS connection. This is only required if the Mobile Security Manager is configured to use mutual authentication.
Trusted Root CA	Click **Add** and the select the root CA certificate that was used to issue the certificate for the interface where the gateway will connect to retrieve HIP reports (this could be a different server certificate than the one issued for the device check-in interface on the Mobile Security Manager).You must import the root CA certificate and add it to this list.

Creating HIP Objects

▶ *Objects > GlobalProtect > HIP Objects*

Use this page to define host information profile (HIP) objects. HIP objects provide the matching criteria to filter out the host information you are interested in using to enforce policy from the raw data reported by the agent/app. For example, while the raw host data may include information about several antivirus packages that are installed on the client, you may only be interested in one particular application that you require within your organization. In this case, you would create a HIP object to match the specific application you are interested in enforcing.

The best way to determine what HIP objects you need is to determine how you will use the host information you collect to enforce policy. Keep in mind that the HIP objects themselves are merely building blocks that allow you to create the HIP profiles that are used in your security policies. 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 client OS. By doing this, you will 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 following tables.

- “General Tab”
- “Mobile Device Tab”
- “Patch Management Tab”
- “Firewall Tab”
- “Antivirus Tab”
- “Anti-Spyware Tab”
- “Disk Backup Tab”
- “Disk Encryption Tab”
- “Data Loss Prevention Tab”
- “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*.

General Tab

Use the **General** tab to specify a name for the new HIP object and to configure the object to match against general host information such as domain, operating system, or the type of network connectivity it has.

Table 216. HIP Object General Settings

Field	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	Select this check box if you want the HIP object to be available to: • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the object will be available only to the vsys selected in the **Objects** tab, **Virtual System** drop-down. For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the HIP Object dialog. • All device groups on Panorama™. If you clear the check box, the object will be available only to the device group selected in the **Objects** tab, **Device Group** drop-down. After you save the object, you cannot change its **Shared** setting. The **Objects > GlobalProtect > HIP Objects** page shows the current setting in the Location field.
Disable override	This check box only appears in Panorama. It controls override access to the HIP object in device groups that are descendants of the **Device Group** selected in the **Objects** tab. Select the check box if you want to prevent administrators from creating local copies of the object in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding is enabled.
Description	Enter an optional description.
Host Info	Select the check box to enable filtering on the host information fields.
Domain	To match on a domain name, choose an operator from the drop-down list 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 a specific OS version from the third drop-down, or select **All** to match on any OS version from the selected vendor.
Client Versions	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.
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**.

Mobile Device Tab

Use the **Mobile Device** tab to enable HIP matching on data collected from mobile devices running the GlobalProtect app.

Table 217. HIP Object Mobile Device Settings

Field	Description
Mobile Device	Select the check box to enable filtering on host data collected from mobile devices that are running the GlobalProtect app. Selecting this check box enables the Device, Settings, and Apps subtabs for editing.
Device subtab	• **Serial Number**—To match on all or part of a device serial number, choose an operator from the drop-down and enter a string to match. • **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 subtab	• **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**. • **Device Managed**—Filter based on whether the device is managed by an MDM. To match devices that are managed, select **yes**. To match devices that are not managed, select **no**. • **Rooted/Jailbroken**—Filter based on whether the device has been rooted or jailbroken. To match devices that have been rooted/jailbroken, select **yes**. To match devices that have not been rooted/jailbroken, select **no**. • **Disk Encryption**—Filter based on whether the device data has been encrypted. To match devices that have disk encryption enabled, select **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 subtab	• **Apps**—(Android devices only) Select this check box 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** subtab – **Has Malware**—To match devices that have malware-infected apps installed select **Yes**; to match devices that do not have malware-infected apps installed, select **No**. If you do not want to use **Has Malware** as match criteria, select **None**. • **Include** subtab – **Package**—To match devices that have specific apps installed, click **Add** and then enter the unique app name (in reverse DNS format; for example, com.netflix.mediaclient) in the **Package** field and enter the corresponding app **Hash**, which the GlobalProtect app calculates and submits with the device HIP report.

Patch Management Tab

Use the **Patch Management** tab to enable HIP matching on the patch management status of the GlobalProtect clients.

Table 218. HIP Object Patch Management Settings

Field	Description
Patch Management	Select the check box to enable matching on the patch management status of the host. Selecting this check box enables the Criteria and Vendor subtabs for editing.
Criteria subtab	Specify the following settings on this subtab: • **Is Enabled**—Match on whether patch management software is enabled on the host. If the **Is Installed** check box is cleared, this field is automatically set to **none** and is disabled for editing. • **Is Installed**—Match on whether patch management software is installed on the host. • **Severity**—Match on whether the host has missing patches of the specified severity level. • **Check**—Match on whether the has missing patches. • **Patches**—Match on whether the host has specific patches. Click **Add** and enter file names for the specific patch names to check for.
Vendor subtab	Use this subtab to define specific patch management software vendors and/or products to look for on the host to determine a match. Click **Add** to and then choose a **Vendor** from the drop-down list. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings.

Firewall Tab

Use the **Firewall** tab to enable HIP matching based on the firewall software status of the GlobalProtect clients.

Table 219. HIP Object Firewall Settings

Field	Description
Firewall	Select the **Firewall** check box to enable matching on the firewall software status of the host: • **Is Enabled**—Match on whether firewall software is enabled on the host. If the **Is Installed** check box is cleared, this field is automatically set to **none** and is disabled for editing. • **Is Installed**—Match on whether firewall software is installed on the host. • **Vendor and Product**—Define specific firewall software vendors and/or products to look for on the host to determine a match.Click **Add** to and then choose a **Vendor** from the drop-down list. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings. • **Exclude Vendor**—Select the check box to match hosts that do not have software from the specified vendor.

Antivirus Tab

Use the **Antivirus** tab to enable HIP matching based on the antivirus coverage on the GlobalProtect clients.

Table 220. HIP Object Antivirus Settings

Field	Description
Antivirus	Select the check box to enable matching on the antivirus coverage on the host: • **Real Time Protection**—Match on whether real-time antivirus protection is enabled on the host. If the **Is Installed** check box is cleared, this field is automatically set to **none** and is disabled for editing. • **Is Installed**—Match on whether antivirus software is installed on the host. • **Virus Definition Version**—Specify whether to match on whether the virus definitions have been updated within a specified number of days or release versions. • **Product Version**—Use this option to match against a specific version of the antivirus software. To specify a version to look for, 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 time that the last antivirus 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 software vendors and/or products to look for on the host to determine a match.Click **Add** to and then choose a **Vendor** from the drop-down list. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings. • **Exclude Vendor**—Select the check box to match hosts that do not have software from the specified vendor.

Anti-Spyware Tab

Use the Anti-Spyware tab to enable HIP matching based on the anti-spyware coverage on the GlobalProtect clients.

Table 221. HIP Object Anti-Spyware Settings

Field	Description
Anti-Spyware	Select the check box to enable matching on the anti-spyware coverage on the host and then define additional matching criteria for the match as follows: • **Real Time Protection**—Match on whether real-time anti-spyware protection is enabled on the host. If the **Is Installed** check box is cleared, this field is automatically set to **none** and is disabled for editing. • **Is Installed**—Match on whether anti-spyware software is installed on the host. • **Virus Definition Version**—Specify whether to match on whether the virus definitions have been updated within a specified number of days or release versions. • **Product Version**—Use this option to match against a specific version of the anti-spyware software. To specify a version to look for, 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 time that the last 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 anti-spyware software vendors and/or products to look for on the host to determine a match. Click **Add** to and then choose a **Vendor** from the drop-down list. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings. • **Exclude Vendor**—Select the check box to match hosts that do not have software from the specified vendor.

Disk Backup Tab

Use the **Disk Backup** tab to enable HIP matching based on the disk backup status of the GlobalProtect clients.

Table 222. HIP Object Disk Backup Settings

Field	Description
Disk Backup	Select the check box 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/or products to look for on the host to determine a match. Click **Add** to and then choose a **Vendor** from the drop-down list. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings. • **Exclude Vendor**—Select the check box to match hosts that do not have software from the specified vendor.

Disk Encryption Tab

Use the **Disk Encryption** tab to enable HIP matching based on the disk encryption status of the GlobalProtect clients.

Table 223. HIP Object Disk Encryption Settings

Field	Description
Disk Encryption	Select the check box to enable matching on the disk encryption status on the host:
Criteria	Specify the following settings on this subtab: • **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	Use this subtab to define specific disk encryption software vendors and/or products to look for on the host to determine a match. Click **Add** to and then choose a **Vendor** from the drop-down list. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings and return to the **Disk Encryption** tab.

Data Loss Prevention Tab

Use the **Data Loss Prevention** tab enable HIP matching based on whether or not the GlobalProtect clients are running data loss prevention software.

Table 224. HIP Object Data Loss Prevention Settings

Field	Description
Data Loss Prevention	Select the check box 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 Enabled**—Match on whether DLP software is enabled on the host. If the **Is Installed** check box is cleared, this field is automatically set to **none** and is disabled for editing. • **Is Installed**—Match on whether DLP software is installed on the host. • **Vendor and Product**—Define specific DLP software vendors and/or products to look for on the host to determine a match. Click **Add** to and then choose a **Vendor** from the drop-down list. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings. • **Exclude Vendor**—Select the check box to match hosts that do not have software from the specified vendor.

Custom Checks Tab

Use 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 "Setting Up the GlobalProtect Portal".

Table 225. HIP Object Custom Checks Settings

Field	Description
Custom Checks	Select the check box to enable matching on any custom checks you have 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 agent checks for running processes; if you just want to check if a specific process is present on the system, clear the **Running** check box.
Registry Key	To check Windows hosts for a specific registry key, click **Add** and enter the **Registry Key** to match on. To only match hosts that do not have the specified registry key, select the **Key does not exist or match the specified value data** check 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 the **Negate** check box. Click **OK** to save the settings.
Plist	To check Mac hosts for a specific Property List (plist), click **Add** and enter the **Plist** name. To only match hosts that do not have the specified plist, select the **Plist does not exist** check box. 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 and/or value, select the **Negate** check box. Click **OK** to save the settings.

Setting Up HIP Profiles

▶ *Objects > GlobalProtect > HIP Profiles*

Use this page to create the HIP profiles you will use to set up HIP-enabled security polices. A collection of HIP objects that are to be evaluated together, either for monitoring or for security policy enforcement. When you create your HIP profiles, you can combine the HIP objects you previously created (as well as other HIP profiles) using Boolean logic such that when a traffic flow is evaluated against the resulting HIP profile it will either match or not match. If there is a match, the corresponding policy rule will be enforced; if there is not a match, the flow will be 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 on 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*.

Table 226. HIP Profile Settings

Field	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	Enter an optional description.
Shared	Select this check box if you want the HIP profile to be available to: • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the **Objects** tab, **Virtual System** drop-down. For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the HIP Profile dialog. • All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the **Objects** tab, **Device Group** drop-down. After you save the profile, you cannot change its **Shared** setting. The **Objects > GlobalProtect > HIP Profiles** page shows the current setting in the Location field.

Table 226. HIP Profile Settings (Continued)

Field	Description
Disable override	This check box only appears in Panorama. It controls override access to the HIP profile in device groups that are descendants of the **Device Group** selected in the **Objects** tab. Select the check box if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. The check box is cleared by default, which means overriding 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 click add ⊞ to move it over to the **Match** text box on the HIP Profile 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 the **NOT** check box before adding the object. Continue adding match criteria as appropriate for the profile you are building, making sure to select the appropriate Boolean operator radio button (**AND** or **OR**) between each addition (and, again, using the **NOT** check box when appropriate). If you are creating 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 logic you intend. For example, the following expression indicates that the HIP profile will match traffic from a host that has either FileVault disk encryption (for Mac OS systems) or TrueCrypt disk encryption (for 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/profiles to the new HIP profile, click **OK**.

Setting Up and Activating the GlobalProtect Agent

▶ *Device > GlobalProtect Client*

Use this page to download the GlobalProtect agent software to the firewall hosting the portal and activate it so that clients connecting to the portal can download it. You define how and when the software downloads occur—whether upgrades occur automatically when the agent connects, whether end users are prompted to upgrade, or whether upgrade is allowed at all for a particular set of users—in the client configurations you define on the portal. See the description of the Agent Upgrade field in the section that describes the portal “Client Configuration Tab” for more details. For details on the various options for distributing the GlobalProtect agent software and for step-by-step instructions for deploying the software, refer to “Deploy the GlobalProtect Client Software” in the *GlobalProtect Administrator’s Guide*.

For initial download and installation of the GlobalProtect agent, the user on the client system must be logged in with administrator rights. For subsequent upgrades, administrator rights are not required.

The following table provides help for using this screen. For more detailed information on deploying agent software, refer to the *GlobalProtect Administrator's Guide*.

Table 227. GlobalProtect Client Settings

Field	Description
Version	The version number of the GlobalProtect agent software that is available on the Palo Alto Networks Update Server. To check if a new agent software release is available from Palo Alto Networks, click **Check Now**. The firewall will use its service route to connect to the Update Server to check for new versions and, if there are updates available, display them at the top of the list.
Size	The size of the agent 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 agent software package has been downloaded to the firewall.
Currently Activated	A check mark in this column indicates that the corresponding version of the agent software has package has been activated on the firewall and can be downloaded by connecting agents. Only one version of the software can be activated at a time.
Action	Indicates the current action you can take for the corresponding agent software package as follows: • **Download**—The corresponding agent software version is available on the Palo Alto Networks Update Server. Click the link to initiate the download. If the firewall does not have access to the Internet, use an Internet-connected computer to go to the Software Update site to look for and **Download** new agent software versions to your local computer. Then click the **Upload** button on the GlobalProtect Client screen to manually upload the agent software to the firewall. • **Activate**—The corresponding agent software version has been downloaded to the firewall, but agents cannot yet download it. Click the link to activate the software and enable agent upgrade. To activate a software update that you manually uploaded to the firewall using the **Upload** button, you must click **Activate From File** button and select the version you want to activate from the drop-down (you may then need to refresh the screen for it to display as **Currently Activated**). • **Reactivate**—The corresponding agent software has been activated and is ready for client download. Because only one version of the GlobalProtect agent 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 will 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 agent version.
☒	Remove the previously downloaded agent software image from the firewall.

Setting Up the GlobalProtect Agent

The GlobalProtect agent (PanGP Agent) is an application that is installed on the client system (typically a laptop) to support GlobalProtect connections with portals and gateways and is supported by the GlobalProtect service (PanGP Service).

Make sure that you choose the correct installation option for your host operating system (32-bit or 64-bit). If installing on a 64-bit host, use 64-bit browser/Java combo for the initial installation.

To install the agent, open the installer file and follow the on-screen instructions.

To configure the agent:

1. Choose **Start > All Programs > Palo Alto Networks > GlobalProtect > GlobalProtect**.

   The client interface opens to show the **Settings** tab.

2. Specify the username and password to use for GlobalProtect authentication, and optionally select the **Remember Me** check box.

3. Enter the IP address of the firewall that serves as the GlobalProtect Portal.

4. Click **Apply**.

Using the GlobalProtect Agent

The tabs in the GlobalProtect agent contain useful information about status and settings, and provide information to assist in troubleshooting connection issues.

- **Status tab**—Displays current connection status and lists any warnings or errors.
- **Details tab**—Displays information about the current connection, including portal IP addresses and protocol, and presents byte and packet statistics about the network connection.
- **Host State tab**—Displays the information stored in the HIP. Click a category on the left side of the window to display the configured information for that category on the right side of the window.
- **Troubleshooting tab**—Displays information to assist in troubleshooting.
  - **Network Configurations**—Displays the current client 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 you to display logs for the GlobalProtect agent (PanGP Agent) and service (PanGP Service). Choose the log type and debugging level. Click **Start** to begin logging and **Stop** to terminate logging.

Chapter 10

Configuring Quality of Service

This section describes how to configure quality of service (QoS) on the firewall. Refer to each topic in the table below for details on configuring the components that support a complete QoS implementation. After setting up QoS, you can also monitor traffic receiving QoS treatment.

What are you looking for?	**See**
Define traffic to receive QoS treatment and assign it a QoS class of service.	▶ *“Defining a QoS Policy”*
Define QoS classes of service, setting bandwidth limitations and priority for each class.	▶ *“Defining a QoS Profile”*
Enable QoS on an interface.	▶ *“Enabling QoS for Firewall Interfaces”*
Monitor traffic receiving QoS treatment.	▶ *“Monitoring a QoS Interface”*
Looking for more?	**See** Quality of Service**.**

Defining a QoS Profile

▶ *Network > Network Profiles > QoS Profiles*

For each interface, you can define QoS profiles that determine how the QoS traffic classes are treated. You can set overall limits on bandwidth regardless of class and also set limits for individual classes. You can also assign priorities to different classes. Priorities determine how traffic is treated in the presence of contention.

Click **Add** and complete the fields described in to define a QoS profile.

Refer to "Enabling QoS for Firewall Interfaces" for information on configuring firewall interfaces for QoS and refer to "QoS Statistics" to configure the policies that will activate the QoS restrictions.

Table 228. QoS Profile Settings

Field	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.
Egress Max	Enter the maximum bandwidth allowed for this profile (Mbps). The Egress Max value for a QoS profile must be less than or equal to the Egress Max value defined for the physical interface that QoS is enabled on. See "Enabling QoS for Firewall Interfaces" . **Note:** *Though this is not a required field, it is recommended to always define the Egress Max value for a QoS profile.*
Egress Guaranteed	Enter the bandwidth that is guaranteed for this profile (Mbps).
Classes	Click **Add** to 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 • **Egress Max**—Click and enter the bandwidth limit (Mbps) for this class. The Egress Max value for a QoS class must be less than or equal to the Egress Max value defined for the QoS profile. **Note:** *Though this is not a required field, it is recommended to always define the Egress Max value for a QoS profile.* **Egress Guaranteed**—Click and enter the guaranteed bandwidth (Mbps) for this class.When contention occurs, traffic that is assigned a lower priority is dropped. Real-time priority uses its own separate queue.

Defining a QoS Policy

▶ *Policies > QoS*

The QoS policy determines how traffic is classified for treatment when it passes through an interface with QoS enabled. For each rule, specify one of eight classes. You can also assign a schedule to specify which rule is active. Unclassified traffic is automatically assigned to class 4.

For information on defining policies on Panorama™, see "Defining Policies on Panorama".

Click **Add** to open the **QoS Policy Rule** dialog. The **QoS Policy Rule** dialog contains six subtabs, described in Table 229:

- "General Tab"
- "Source Tab"
- "Destination Tab"
- "Application Tab"
- "Service/ URL Category Tab"
- "DSCP/TOS Tab"
- "Other Settings Tab"

Refer to "Enabling QoS for Firewall Interfaces" for information on configuring firewall interfaces for QoS and refer to "QoS Statistics" for information on configuring classes of service.

Use the QoS Policy page to perform several actions, including:

- To view just the rules for a specific virtual system, select the system from the **Virtual System** drop-down list and click **Go**.
- To apply a filter to the list, select from the **Filter Rules** drop-down list.
- To view just the rules for specific zones, select a zone from the **Source Zone** and/or **Destination Zone** drop-down lists, and click **Filter by Zone**.

Shared polices pushed from Panorama are shown in green and cannot be edited at the device level.

- To add a new QoS rule, do one of the following:
  – Click **Add** at the bottom of the page and configure the rule. A new rule is added to the bottom of the list.
  – Select **Clone Rule**, or select a rule by clicking the white space of the rule, and select **Clone** at the bottom of the page (a selected rule has a yellow background). The copied rule is inserted below the selected rule.

Table 229. QoS Rule Settings

Field	Description
General Tab	
Name	Enter a name to identify the rule (up to 31 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, click **Add** to 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.
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).
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 list and do any of the following: • Select the check box 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 will set the check box 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 the appropriate check boxes in the **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, refer to "Defining Address Groups" .
Source User	Specify the source users and groups to which the QoS policy will apply.
Negate	Select the check box 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).

Table 229. QoS Rule Settings (Continued)

Field	Description
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 list and do any of the following: • Select the check box 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 will set the check box 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 the appropriate check boxes in the **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** (refer to "Defining Applications"). To define new address groups, refer to "Defining Address Groups" .
Negate	Select the check box to have the policy apply if the specified information on this tab does NOT match.
Application Tab	
Application	Select specific applications for the QoS rule. To define new applications, refer to "Defining Applications" . To define application groups, refer to "Defining Application Groups" . 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 Object tabs.
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 list: • **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. Refer to "Services" and "Service Groups" .

Table 229. QoS Rule Settings (Continued)

Field	Description
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 list. You can add multiple categories. Refer to "Dynamic Block Lists" for information on defining custom categories.
DSCP/TOS Tab	match the QoS rule to traffic with any DSCP marking/classification, or select a specific codepoint to match to traffic
Any	Select the option **Any** (the default setting) 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**. • 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 "QoS Statistics" for information on configuring settings for QoS classes.
Schedule	Choose the calendar icon to set a schedule for the QoS policy to apply.

Enabling QoS for Firewall Interfaces

▶ *Network > QoS*

Use the **QoS** page to set bandwidth limits for an interface and enable the interface to enforce Quality of Service (QoS) for egress traffic. Enabling a QoS interface includes attaching a QoS profile to the interface.

What are you looking for?	See
Tell me about QoS on a Palo Alto Networks next-generation firewall.	▶ *“QoS Overview”*
What do I need to do before I can enable a QoS on an interface?	Define traffic to receive a QoS class of service based on traffic source, destination, application, and/or a DSCP value: ▶ *“Defining a QoS Policy”* Define QoS classes of service, including setting maximum and/or guaranteed bandwidth and priority (real-time, high, medium, or low) for each class of service: ▶ *“Defining a QoS Profile”*
What are the fields available to enable QoS on an interface?	▶ *“Enabling QoS on an Interface”*
After setting up a QoS interface, how can I continue to monitor traffic receiving QoS treatment?	▶ *“Monitoring a QoS Interface”*
Looking for more?	**See** Quality of Service**.**

QoS Overview

Quality of Service (QoS) allows you to guarantee bandwidth and priority to specific flows in network traffic. A QoS implementation on a Palo Alto Networks next-generation firewall requires three components:

- **QoS policy rule** - Define a QoS Policy rule to match to traffic based on the traffic source, destination, application, and/or Differentiated Services Codepoint (DSCP). Traffic matched to the QoS policy rule is assigned a QoS class of service to receive (**Policies > QoS**).
- **QoS profile** - Create a QoS profile to define bandwidth and priority for each QoS class of service (**Network > Network Profiles > QoS Profile**). You can define a guaranteed or maximum bandwidth for each class of service, as well as define the class to receive real-time, high, medium, or low priority.
- **QoS interface** - Enable QoS on an interface to allow traffic to be shaped and prioritized as it egresses that interface (**Network > QoS**). You can also enable QoS on an interface in order to limit or guarantee bandwidth for that interface.

Enabling QoS on an Interface

▶ *Network > QoS*

Add or modify a QoS Interface. QoS is supported on physical interfaces and, depending on firewall platform, 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 platform.

Table 230. QoS Interface Settings

Field	Configured In	Description
Interface Name	**QoS Interface > Physical Interface**	Select the firewall interface on which to enable QoS.
Egress Max (Mbps)		Enter the limit on traffic leaving the firewall through this interface. **Note:** *Though this is not a required field, it is recommended to always define the Egress Max value for a QoS interface.*
Turn on QoS feature on this interface		Select the check box to enable QoS on the selected interface.
Clear Text 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 “QoS Statistics”.
Tunnel Interface		
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 limit on clear text or tunneled traffic leaving the firewall through this interface.

Table 230. QoS Interface Settings

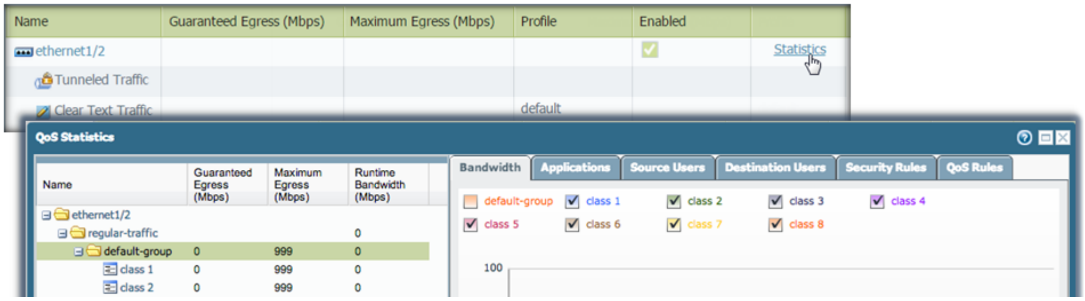
Field	Configured In	Description
Add		• Click **Add** on the **Clear Text Traffic** tab to define additional granularity to the treatment of clear text traffic. Click individual entries to configure the following settings: – **Name**—Enter a name to identify these settings. – **QoS Profile**—Select the QoS profile to apply to the specified interface and subnet. For instructions on defining QoS profiles, refer to “QoS Statistics” . – **Source Interface**—Select the firewall interface. – **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, select the check box for the entry and click **Delete**. 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.

Monitoring a QoS Interface

▶ *Network > QoS*

Select the Statistics link to view bandwidth, session, and application information for configured QoS interfaces. The left panel shows the QoS tree table, and the right panel shows data in the following tabs:

Table 231. QoS Statistics



Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Profile	Enabled	
ethernet1/2				✓	Statistics
Tunneled Traffic					
Clear Text Traffic			default		

QoS Statistics

Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Runtime Bandwidth (Mbps)
ethernet1/2			
regular-traffic			0
default-group	0	999	0
class 1	0	999	0
class 2	0	999	0

Field	Description
Bandwidth	Shows the real time bandwidth charts for the selected node and classes. This information is updated every two seconds. **Note:** *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.

Chapter 11

Central Device Management Using Panorama

Panorama™, available both as a dedicated hardware platform and as a VMware virtual appliance, is the centralized management system for the Palo Alto Networks® family of next-generation firewalls. It shares the same web-based look and feel as the individual firewall interface, and allows you to seamlessly transition in to managing the firewalls centrally and reducing the administrative effort in managing multiple firewalls.

This section serves as a field reference for using the Panorama web interface to manage the firewalls on your network. For information on setting up Panorama, Panorama concepts and workflows, refer to the Panorama Administrator's Guide.

- "Panorama Tab"
- "Switching Device Context"
- "Setting Up Storage Partitions"
- "Configuring High Availability (HA)"
- "Managing Devices"
- "Backing Up Firewall Configurations"
- "Defining Device Groups"
- "Defining Panorama Administrator Roles"
- "Creating Panorama Administrative Accounts"
- "Specifying Panorama Access Domains for Administrators"
- "Committing your Changes in Panorama"
- "Managing Templates and Template Stacks"
- "Logging and Reporting"
- "Enable Log Forwarding"
- "Managing Log Collectors"
- "Defining Log Collector Groups"
- "Generating User Activity Reports"
- "Managing Device Updates and Licenses"

- "Scheduling Dynamic Updates"
- "Scheduling Configuration Exports"
- "Upgrading the Panorama Software"
- "Register VM-Series Firewall as a Service on the NSX Manager"

Panorama Tab

▶ *Panorama*

The **Panorama** tab is similar to the **Devices** tab for the firewall, but the settings apply to the Panorama server, not the managed firewalls. The following table describes the pages on this tab. To access a page, click the page name link on the side menu.

Table 232. Summary of Panorama Pages

Page	Description
Setup	Allows you to specify the Panorama host name, the network settings of the management interface, and the addresses of network servers (DNS and NTP). Refer to "Defining Management Settings".
Templates	Allows you to create templates and template stacks to manage configuration options based on the **Device** and **Network** tabs. "Managing Templates and Template Stacks" enable you to reduce the administrative effort in deploying multiple firewalls with similar configurations.
Config Audit	Allows you to view and compare configuration files. Refer to "Defining Operations Settings"and "Switching Device Context".
Managed Devices	Allows you to add firewalls for management by Panorama, push shared configuration to managed firewalls, and run comprehensive configuration audits on firewalls or entire device groups. Refer to "Managing Devices".
Device Groups	Allows you to group firewalls based on function, network segmentation, or geographic location. A device group 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. See "Defining Device Groups".
Managed Collectors	Allows you to configure and manage Log Collectors. A Log Collector can be local to an M-Series appliance in Panorama mode (default Log Collector) or it can be an M-Series appliance in Log Collector mode (dedicated Log Collector). An M-Series appliance in Panorama mode or a Panorama virtual appliance can manage a Log Collector. Because you use Panorama to configure Log Collectors, they are also called Managed Collectors. Managed firewalls running PAN-OS® 5.0 and later releases can send logs to Managed Collectors. You can also use this tab to upgrade the software on your Log Collectors: first download the latest Panorama software and then push it to your Log Collectors by clicking **Install** on the Managed Collectors page. **Note:** *An M-Series appliance can be a Panorama management server, a Log Collector, or both. The operational command to change the mode of an M-Series appliance is* **`request system system-mode [panorama	logger]`**. *To view the current mode, run* **`show system info	match system-mode`**. *When an M-Series appliance is in Log Collector mode, only the CLI is available for management.* For details, see "Managing Log Collectors".

Table 232. Summary of Panorama Pages (Continued)

Page	Description
Collector Groups	Allows you to logically group up to eight Log Collectors so you can apply the same configuration settings to all Log Collectors in a Collector Group and then assign firewalls to the Log Collectors. Panorama uniformly distributes the logs among all the disks in a Log Collector and across all members in the Collector Group. Each Panorama can have up to 16 Collector Groups. For details, see "Defining Log Collector Groups".
Admin Roles	Allows you to specify the privileges and responsibilities that are assigned to users who require access to Panorama. Refer to "Defining Panorama Administrator Roles".
Password Profiles	Allows you to define password profiles, which can then be applied to Panorama administrators. You can configure the following profile options: • Required password change period (days) • Expiration warning period (days) • Post Expiration Admin Login Count • Post Expiration Grace Period (days)
Administrators	Allows you to define the accounts for users who require access to Panorama. See "Creating Panorama Administrative Accounts". **Note:** *If a user account is locked out, the **Administrators** page displays a lock icon in the Locked User column. You can click the icon to unlock the account.*
High Availability	Allows you to configure a pair of Panorama devices to support high availability (HA). See "Configuring High Availability (HA)".
Certificate Management	Allows you to configure and manage certificates, certificate profiles, and keys. See "Managing Device Certificates".
Log Settings	Allows you to define Simple Network Management Protocol (SNMP) trap receivers, syslog servers, and email addresses for distributing log messages.
Server Profiles	Allows you to specify profiles for servers that provide services to Panorama. See the following sections: • "Configuring Email Notification Settings" • "Configuring SNMP Trap Destinations" • "Configuring Syslog Servers" • "Configuring RADIUS Server Settings" • "Configuring TACACS+ Server Settings" • "Configuring LDAP Server Settings" • "Configuring Kerberos Server Settings".
Authentication Profile	Allows you to specify a profile for authenticating access to Panorama. See "Setting Up Authentication Profiles".
Authentication Sequence	Allows you to specify a series of authentication profiles to use for permitting access to Panorama. See "Setting Up an Authentication Sequence".
Access Domain	Access Domains enable you to control administrator access to device groups, templates, template stacks, and the web interface of devices ("Switching Device Context"). See "Specifying Panorama Access Domains for Administrators".

Table 232. Summary of Panorama Pages (Continued)

Page	Description
Scheduled Config Export	Allows you to collect running configurations from Panorama and managed firewalls and deliver them daily to a File Transfer Protocol (FTP) server or by using Secure Copy (SCP) to securely transfer data between the Panorama server and a remote host. See “Scheduling Configuration Exports”.
Software	Allows you to view the available Panorama software releases and download and install a selected software version. Refer to “Upgrading the Panorama Software”.
Dynamic Updates	Allows you to view the latest application definitions and information on new security threats, such as antivirus signatures (threat prevention license required) and update Panorama with the new definitions. Refer to “Updating Threat and Application Definitions”.
Support	Allows you to access product and security alerts from Palo Alto Networks. Refer to “Viewing Support Information”.
Device Deployment	Allows you to view current license information on the managed firewalls and install software, clients, and dynamic content on the managed firewalls and managed collectors. Refer to “Managing Device Updates and Licenses”. To automate the process of downloading and installing dynamic updates, see “Scheduling Dynamic Updates”.
Master Key and Diagnostics	Allows you to specify a master key to encrypt private keys on the firewall. Private keys are stored in encrypted form by default even if a new master key is not specified. Refer to “Encrypting Private Keys and Passwords on the Firewall”.

Switching Device Context

Switching device context enables you to launch the web interface of a managed firewall from the Panorama web interface so you can directly access and manage firewall-specific settings (such as firewall-specific policies, network settings, and device setup).

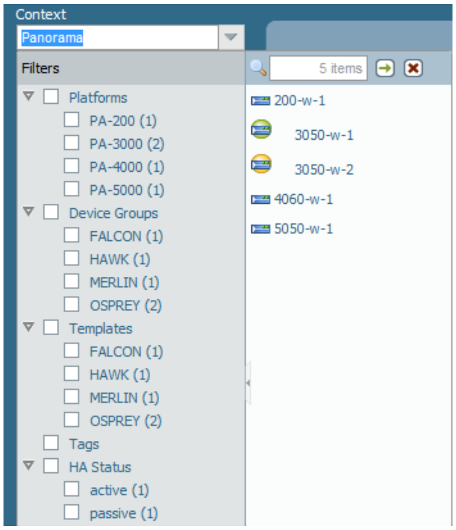
Use the **Context** drop-down above the side menu to choose an individual firewall or the full Panorama view. When you select a firewall, the web interface refreshes to show all the device tabs and options for the selected firewall. The drop-down displays only the firewalls to which you have administrative access (see “Creating Panorama Administrative Accounts”) and that are connected to Panorama. Use the filters to refine your search criteria.

The icons of firewalls that are in high availability (HA) mode will have colored backgrounds to indicate their HA state:

- Green—Active.
- Yellow—Passive or the firewall is initiating (the initiating state lasts for up to 60 seconds after bootup).

- Red—The firewall is non-functional (error state), suspended (an administrator disabled the firewall), or tentative (for a link or path monitoring event in an active/active HA configuration).

Figure 15. Choosing Context



Setting Up Storage Partitions

▶ *Panorama > Setup > Operations > Storage Partition Setup*

By default, the Panorama virtual appliance has a single disk partition for all data in which, regardless of the total disk size, 10.89GB is allocated for log storage. Increasing the disk size doesn't increase the log storage capacity. To modify the log storage capacity, your options are:

- Add another virtual disk of up to 2TB. This option applies to Panorama on a VMware ESXi server and on VMware vCloud Air.
- Mount Panorama to a Network File System (NFS). This option is available only for Panorama on an ESXi server. Click **Storage Partition Setup** in the Miscellaneous section, set the **Storage Partition** to **NFS V3**, and complete the fields in Table 233.
- Revert to the default internal storage partition if you previously configured another virtual disk or mounted to an NFS. This option applies to Panorama on an ESXi server and on vCloud Air. Click **Storage Partition Setup** in the Miscellaneous section and set the **Storage Partition** to **Internal**.

You must reboot the Panorama management server after configuring the storage partition settings. Select **Panorama > Setup > Operations** *and click* **Reboot Panorama***.*

Table 233. Panorama Storage Partition Setup—NFS V3

Field	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.

Table 233. Panorama Storage Partition Setup—NFS V3 (Continued)

Field	Description
Port	Specify the port for communication with the NFS server.
Read Size	Specify the maximum size in bytes (range is 256-32768) for NFS read operations.
Write Size	Specify the maximum size in bytes (range is 256-32768) for NFS write operations.
Copy on Setup	Select the check box to mount the NFS partition and copy any existing logs to the destination directory on the server when Panorama boots.
Test Logging Partitions	Click to perform a test that mounts the NFS partition and presents a success or failure message.

Configuring High Availability (HA)

▶ *Panorama > High Availability*

High availability (HA) allows for redundancy in the event of a failure. For ensuring HA, you can deploy a pair of hardware-based Panorama appliances or a pair of Panorama virtual appliances in a HA peer configuration that provide synchronized connections to the managed firewalls. Among the peers in the HA configuration, one device must be designated as primary and the other as secondary; the primary device will assume the active state and the secondary device will take the passive state, until a monitored metric fails. The peers maintain a heartbeat, or a periodic ICMP ping, to verify operational status. If the active Panorama server becomes unavailable, the passive server takes over temporarily. With preemption enabled, the default setting, when the active Panorama server becomes available again, the passive server relinquishes control and returns to the passive state.

To configure a HA pair of Panorama virtual appliances, you must have two Panorama licenses with unique serial numbers for each virtual instance.

To enable HA on Panorama, configure the followings settings:

Table 234. Panorama HA Settings

Field	Description
Setup	
Enable HA	Select the check box to enable HA.
Peer HA IP Address	Enter the IP address of the MGT interface of the peer.
Enable Encryption	Enable encryption after exporting the HA key from the HA peer and importing it onto this device. The HA key on this device must also be exported from this device and imported on the HA peer. When enabled, the MGT interface encrypts communication between the HA peers. The key import/export is done on the Certificates page. See “Managing Device Certificates”. **Note:** *HA connectivity uses TCP port 28 with encryption enabled and 28769 when encryption is not enabled.*
Monitor Hold Time (ms)	Enter the length of time (ms) that the system will wait before acting on a control link failure (1000-60000 ms, default 3000 ms).

Table 234. Panorama HA Settings (Continued)

Field	Description
Election Settings	
Priority (Only required on virtual Panorama)	Assign a device as **Primary** and the other as **Secondary** in each pair. This primary or secondary configuration determines which peer is designated as the primary recipient for logs sent by the managed firewalls. You can configure Panorama to use the same log external storage facility for the assigned primary and secondary devices (Network File System or NFS option) or configure logging internally. If you use the NFS option, only the primary recipient receives the logs that are sent from the managed firewalls. However, if local logging is enabled, by default the logs are sent to both the primary and the secondary recipient.
Preemptive	Select the check box to enable the primary Panorama device to resume active operation after recovering from a failure. If this setting is off, then the secondary device remains active even after the higher priority device recovers from a failure.
Preemption Hold Time (min)	Enter the time a passive device will wait before taking over as the active device (range 1-60 min, default 1).
Promotion Hold Time (ms)	Enter the time that the secondary device will wait before taking over (range 0-60000 ms, default 2000).
Hello Interval (ms)	Enter the number of milliseconds between the hello packets sent to verify that the other device is operational (ranges 8000-60000 ms, default 8000).
Heartbeat Interval (ms)	Specify how frequently Panorama sends ICMP pings to the HA peer (range 1000-60000 ms, default 1000).
Monitor Fail Hold Up Time (ms)	Specify the interval that Panorama waits following a path monitor failure before attempting to re-enter the passive state (default 0 ms). During this period, the device is not available to take over for the active device in the event of failure.
Additional Master Hold Up Time (ms)	Specify the interval during which the preempting device remains in the passive state before taking over as the active device (default 7000 ms).

Table 234. Panorama HA Settings (Continued)

Field	Description
Path Monitoring	
Enabled	Select the check box to enable path monitoring. Path monitoring enables Panorama to monitor specified destination IP addresses by sending ICMP ping messages to make sure that they are responsive.
Failure Condition	Select whether a failover occurs when any or all of the monitored path groups fail to respond.
Path Groups	Define one or more path groups to monitor specific destination addresses. To add a path group, specify the following and click **Add**: • **Name**—Specify a name for the path group. • **Enabled**—Select the check box to enable the path group. • **Failure Condition—**Select whether a failure occurs when any or all of the specified destination addresses fails to respond. • **Ping interval**—Specify a length of time between ICMP echo messages to verify that the path is up (range 1000-60000 ms, default 5000). • **Destination IPs**—Enter one or more destination addresses to be monitored (multiple addresses must be separated by commas). • **Ping Interval**—Specify the interval between pings that are sent to the destination address (range 1000-60000 milliseconds, default 5000 milliseconds). • **Ping Count**—Specify the number of failed pings before declaring a failure (range 3-10 pings, default 3 pings). To delete a path group, select the group, and click **Delete**.

Managing Devices

▶ *Panorama > Managed Devices*

A Palo Alto Networks firewall that Panorama manages is called a managed device. The **Managed Devices** page enables you to perform administrative tasks on the firewalls and see their status information.

Panorama can manage PAN-OS firewalls running the same major release or earlier supported versions, but not firewalls running a later release version. For example, Panorama 5.0 can manage firewalls running PAN-OS 5.0 or earlier supported versions, but it cannot manage firewalls running PAN-OS 5.1.

Use the **Managed Devices** page to perform the following tasks:

- **Add managed devices—**Click **Add** and enter the serial number of one or more firewalls. Enter only one serial number per row. After adding firewalls as managed devices, to enable Panorama to connect with and manage them, you must add the firewall serial number on the Panorama management server and add the IP address of the Panorama management server on the firewall (see “Defining Management Settings”).

- **Delete managed devices—**Select the check box for one or more firewalls and click **Delete** to remove the firewall from the list of firewalls that Panorama manages.

- **Tag devices—**Select the check box for 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. In places where 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, if you add a tag called branch office, you can filter for all branch office firewalls across your network.
- **Group HA Peers—**Select the **Group HA Peers** check box if you want the **Managed Devices** page to group firewalls that are peers in a high availability (HA) configuration. Each HA pair will then have a single check box. For an active-passive HA configuration, consider adding both firewall peers or virtual systems of the peers (if in Multiple Virtual Systems mode) to the same device group. This enables you to push the configuration to both HA peer firewalls at the same time.
- **Install software or content updates—**Click **Install** and select the following options:

Table 235 Software/Content Update on a Managed Device

Field	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 only lists images that you downloaded or uploaded to Panorama using the **Panorama > Device Deployment** pages.
Devices	Use the Filters to select the firewalls on which you want to install the image.
Upload only to device (do not Install)	Select this option if you want to upload the image on the firewall, but do not want to reboot the firewall now. Until you initiate a reboot, PAN-OS does not install the image.
Reboot device after Install	Select this option if you want to upload and install the software image. PAN-OS reboots the firewall.
Group HA Peers	Select this option if you want the Devices list to group firewalls that are peers in an HA configuration.
Filter Selected	If you want the Devices list to display only specific firewalls, select the corresponding Device Name check boxes and select the **Filter Selected** check box.

The **Managed Devices** page displays the following information for each managed firewall:

Table 236. Status of the Managed Devices

Field	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**. Regardless of whether the column is visible, the page displays devices in clusters according to their device group. Each cluster has a header row that displays the device group name, the total number of assigned devices, the number of connected devices, and the device group path in the hierarchy. For example, **Datacenter (2/4 Devices Connected): Shared > Europe > Datacenter** would indicate that a device group named **Datacenter** 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 firewall hostname or serial number.
Virtual System	Lists the virtual systems available on a firewall that is in Multiple Virtual Systems mode.
Tags	Displays the tags defined for each firewall/virtual system.
Serial Number	Displays the serial number of the firewall.
IP Address	Displays the IP address of the firewall/virtual system.
Template	Displays the template or template stack to which the firewall belongs.

Table 236. Status of the Managed Devices

Field	Description
Status	Device State—Indicates the state of the connection (Connected or Disconnected) between Panorama and the firewall. A VM-Series firewall can have two additional states: • Deactivated—Indicates that you have deactivated a virtual machine either directly on the firewall or using the **Deactivate VMs** link on the **Panorama > Device Deployment > Licenses** page and removed all licenses/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 device is in this state for up to 60 seconds after bootup), non-functional (error state), suspended (an administrator disabled the firewall), or 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.
	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.
Backups	On each commit, PAN-OS automatically sends a configuration backup of the managed firewall to Panorama. You can use the **Manage...** link to view the available configuration backups. To load a version from the list of saved configuration files, click **Load**.

Backing Up Firewall Configurations

▶ *Panorama > Managed Devices*

Panorama automatically saves every configuration change you commit to the managed firewalls. To configure the number of versions to keep on the Panorama device, select **Panorama > Setup > Management**, edit the Logging and Reporting Settings, select the **Log Export and Reporting** tab, and enter a value (default 100) in the **Number of Versions for Config Backups** field.

To manage backups on Panorama, select **Panorama > Managed Devices** and, in the **Backups** column for a device, click **Manage**. A window opens to show the saved and committed configurations for the device. Click a **Load** link to restore the backup to the candidate configuration, and then make any desired changes and click **Commit** to restore the loaded configuration to the device. To remove a saved configuration, click the ☒ icon.

Defining Device Groups

▶ *Panorama > Device Groups*

Device groups comprise firewalls and/or virtual systems that 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 each group as a single unit when applying policies. A firewall can belong to only one device group. 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 to implement a layered approach for managing policies across the 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 it inherits policies and objects. At the top level, a device group can have child, grandchild, and great-grandchild device groups—collectively called *descendants*. The Name column in the **Device Groups** page reflects the hierarchy.

Use the **Device Groups** page to add (up to 256), edit, delete, or view device groups. After adding, editing, or deleting a device group, you must commit your changes to Panorama and to the device group: Panorama pushes the configuration changes to the firewalls that are assigned to the device group. For details, see “Committing your Changes in Panorama”.

To edit a device group, click its Name and modify the fields described in the following table.

To add a device group, click **Add** and complete the fields described in the following table.

To delete a device group, select the check box beside its Name and click **Delete**.

Table 237. Device Group Settings

Field	Description
Name	Enter a name to identify the group (up to 31 characters). The name is case-sensitive and must be unique across the entire device group hierarchy. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the device group.
Devices	Select the check box for 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 do not need to assign devices to it.
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. For the rules that govern device group assignments, refer to the Panorama Administrator’s Guide.

Table 237. Device Group Settings (Continued)

Field	Description
Master Device	Select the one firewall in the device group from which Panorama will collect User-ID™ information for use in policies. The gathered user and group mapping information is specific to the device group.
Group HA Peers	Select the check box 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.
Filter Selected	If you want the Devices list to display only specific firewalls, select the corresponding firewall Name check boxes and select the **Filter Selected** check box.

Shared Objects and Policies

Device groups automatically inherit the policies and objects of the Shared location and of ancestor device groups.

- To create a shared policy, select the **Policies** tab, select **Shared** in the **Device Group** drop-down at the top of the tab, select the policy type (for example, **Security > Pre Rules**), and click **Add**. To create a policy that is specific to a particular device group and its descendant device groups, select the appropriate **Device Group** from the drop-down before clicking **Add**.

- To create a shared object, select the **Objects** tab, click **Add**, and select the **Shared** check box. To create an object that is specific to a particular device group and its descendant device groups, select the appropriate **Device Group** from the drop-down before clicking **Add** (do not select **Shared**). By default, overriding the ancestor configuration is enabled for new objects. To disable overriding for the object, select the **Disable override** check box.

If you have objects of the same name and type where one is inherited and another is specific to a device group, by default all the configurations in that device group will use the values of the object that is specific to the device group. If you want the configurations in this scenario to use the values of the inherited object, select ***Panorama > Setup > Management****, edit the Panorama Settings, and select the* ***Ancestor Objects Take Precedence*** *check box.*

If you want an object to have different settings in a descendant device group than in the ancestor from which the object is inherited, you can override the ancestor configuration (see "Overriding or Reverting an Object"). However, you cannot override Shared or default (Predefined) objects.

Applying Policy to Specific Devices in a Device Group

By default, a policy rule applies to all the firewalls in the device group to which the rule is assigned. If you want a rule to apply only to targeted firewalls in the device group, select the policy type in the **Policies** tab, click a **Target** column entry for the desired rule, clear the **Any (target to all devices)** check box, and select the check boxes of the targeted firewalls. To apply the rule to all firewalls in a device group except the targeted firewalls, select the **Target to all but these specified devices** check box. If the list of firewalls is long, you can filter it by **Device State**, **Platforms**, **Device Groups**, **Templates**, **Tags**, and **HA Status**. For firewalls in a high availability (HA) configuration, you can also **Group HA Peers**. To display only the selected firewalls, select the **Filter Selected** check box.

Defining Panorama Administrator Roles

▶ *Panorama > Admin Roles*

Use the **Admin Roles** page to define role profiles that determine the access and responsibilities available to administrative users. For each role, you can configure access on a per feature basis. The set of features that are available for configuring depends on the role scope: custom **Panorama** roles have a larger set (for example, CLI access) than **Device Group and Template** roles. For Device Group and Template administrators, you associate each role with an access domain. For details on assigning roles and access domains, see “Creating Panorama Administrative Accounts”. For details on access domains, see “Specifying Panorama Access Domains for Administrators”.

If you use a RADIUS server to authenticate administrators, map the administrator roles and access domains to RADIUS Vendor Specific Attributes (VSAs).

Table 238. Panorama Administrator Role Settings

Field	Description
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	Enter an optional description of the role.
Role	Select the scope of administrative responsibility: **Panorama** or **Device Group and Template**. The Panorama Administrator's Guide lists the access privileges available for each role.
Web UI	Click the icons for the web interface pages to specify the type of access permitted in the Panorama context (Web UI list) and device context (Context Switch UI list): • Read/write (**Enable**) • **Read Only** • No access (**Disable**)
XML API (Panorama role only)	Select the type of access for the XML API: • **Report**—Access to the firewall reports. • **Log**—Access to the firewall logs. • **Configuration**—Permissions to retrieve or modify the firewall configuration. • **Operational Requests**—Permissions to run operational commands. • **Commit**—Permissions to commit the configuration. • **User-ID Agent**—Access to the User-ID Agent. • **Export**—Permissions to export files from the firewall, including the configuration, block or response pages, certificates, keys, and more. • **Import**—Permissions to import files to the firewall, including software, content, license, configuration, certificates, block pages, custom logs, and more.
Command Line (Panorama role only)	Select the type of role for CLI access: • **None**—Access to the firewall CLI not permitted. • **superuser**—Full access to the current firewall. • **superreader**—Read-only access to the current firewall. • **panorama-admin**—Full access to a selected firewall, except for defining new accounts or virtual systems.

Creating Panorama Administrative Accounts

▶ *Panorama > Administrators*

Administrator accounts define role and authentication parameters. These parameters control access to Panorama and, through context switching, managed firewalls. The predefined **admin** account has full access to Panorama and the managed firewalls. For details on roles, see "Defining Panorama Administrator Roles".

Panorama supports the following authentication options:

- 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 (see "Setting Up Authentication Profiles"), authentication sequences (see "Setting Up an Authentication Sequence"), or for local database authentication.
- Client certificate authentication (web)—This authentication requires no username or password; the certificate suffices to authenticate access to Panorama. See "Using Certificates".
- Public key authentication (SSH)—The administrator generates a public/private key pair on the machine that requires access to Panorama and then uploads the public key to Panorama to allow secure access without requiring the administrator to enter a username and password.

Table 239. Administrator Account Settings

Field	Description
Name	Enter a login username for the administrator (up to 15 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.
Authentication Profile	Select an authentication profile or sequence to authenticate this administrator. You can use this setting for RADIUS, TACACS+, LDAP, Kerberos, or local database authentication.
Use only client certificate authentication (Web)	Select the check box to use client certificate authentication for web access. If you select this check box, a username (**Name**) and **Password** are not required; the certificate suffices to authenticate access to Panorama.
Password/Confirm Password	Enter and confirm a case-sensitive password for the administrator (up to 15 characters). To ensure security, it is recommended that administrators change their passwords periodically using a combination of lower-case letters, upper-case letters, and numbers. You can also set password expiration parameters by selecting a **Password Profile** and/or setting Minimum Password Complexity parameters (see "Defining Management Settings"). Panorama administrators with certain role profiles cannot access the **Panorama > Administrators** page. To change their local password, these administrators can click their username beside the **Logout** link at the bottom of the web interface.
Use Public Key Authentication (SSH)	Select the check box to use SSH public key authentication. Click **Import Key** and **Browse** to select the public key file. 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 (768-4096 bits). **Note:** *If public key authentication fails, Panorama presents a login and password prompt.*

Table 239. Administrator Account Settings (Continued)

Field	Description
Administrator Type	The type selection determines the administrator role options: • **Dynamic**—These roles provide access to Panorama and managed devices. When new features are added, Panorama automatically updates the definitions of dynamic roles; you never need to manually update them. • **Custom Panorama Admin**—These are configurable roles that have read-write access, read-only access, or no access to Panorama features. • **Device Group and Template Admin**—These are 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 pre-configured 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 device administrators and roles. – Export, validate, revert, save, load, or import a configuration in the **Device > Setup > Operations** page. – Configure **Scheduled Config Export** functionality in the **Panorama** tab.
Profile (**Custom Panorama Admin** administrator type)	Select a custom Panorama role (see “Defining Panorama Administrator Roles”).
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, click **Add**, select an **Access Domain** from the drop-down (see “Specifying Panorama Access Domains for Administrators”), and then click the adjacent Admin Role cell and select a custom Device Group and Template administrator role from the drop-down (see “Defining Panorama Administrator Roles”). When administrators 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. **Note:** *If you use a RADIUS server to authenticate administrators, you must map administrator roles and access domains to RADIUS Vendor Specific Attributes (VSAs). Because VSA strings support a limited number of characters, if you configure the maximum number of access domain/role 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 the password profile (see “Defining Password Profiles”), if applicable.

*On the Panorama **Administrators** page, the **Locked User** column displays a lock icon if an account is locked out. The superuser or the Panorama administrator can click the icon to unlock the account.*

Specifying Panorama Access Domains for Administrators

▶ ***Panorama > Access Domain***

Use the **Access Domain** page to provide Device Group and Template administrators access to:

- Device groups—Administrators can manage the policies and objects, and monitor the reports and logs, of firewalls in the device groups that you add to the access domain.
- Templates—Administrators can manage the device and network settings of the firewalls assigned to the templates that you add to the access domain.
- Firewall web interfaces—Administrators can switch to the device context of the firewalls that you add to the access domain.

An administrator with multiple access domains can filter the configuration and monitoring data that the web interface displays by selecting an **Access Domain** from the drop-down at the bottom of the interface. You can define up to 4,000 access domains and manage them locally or using RADIUS Vendor-Specific Attributes (VSAs).

If you use a RADIUS server to authenticate administrators, you must map administrator roles and access domains to RADIUS Vendor Specific Attributes (VSAs).

Table 240. Access Domain Settings

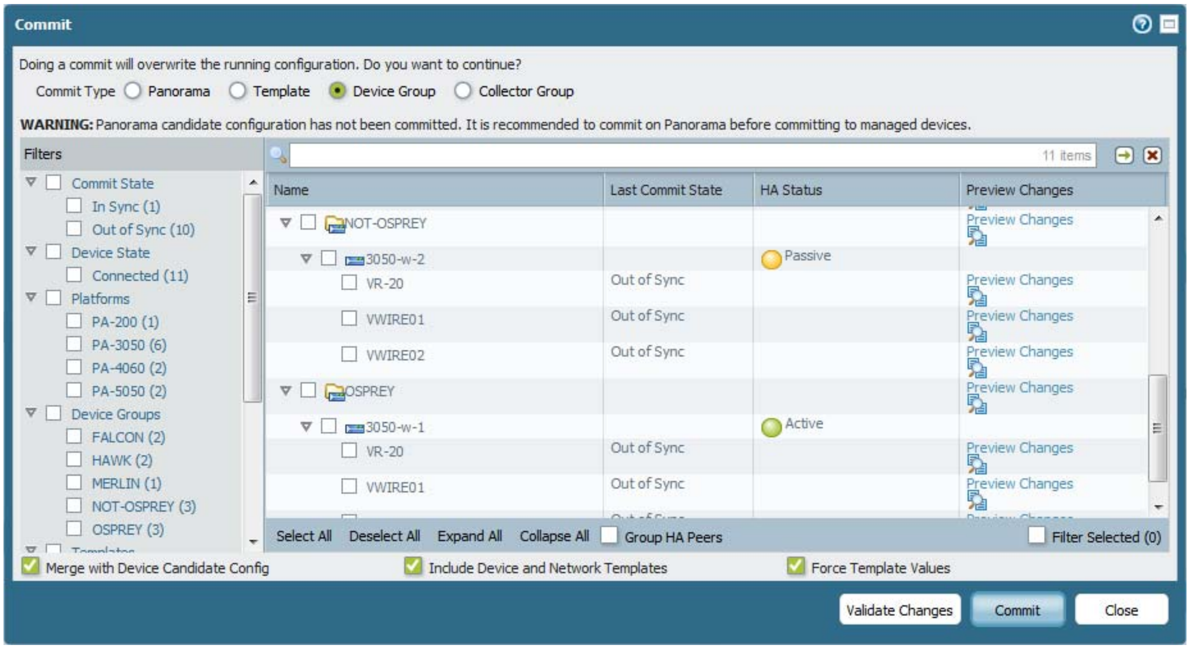
Field	Description
Name	Enter a name for the access domain (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.
Shared Objects	Select one of the following access privileges for the objects that device groups in this access domain inherit 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	Click the icons to enable read-write access for 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. **Note:** *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 check boxes of the firewalls to which the administrator can switch context to perform local configuration edits. If the list is long, you can filter by **Device State**, **Platforms**, **Device Groups**, **Templates**, **Tags**, and **HA Status**.

Committing your Changes in Panorama

To commit Panorama configuration changes, click the **Commit** icon/link to open the commit dialog. This dialog enables you to commit specific areas of the Panorama environment.

You must commit changes to Panorama before committing changes to managed firewalls or managed collectors.

Figure 16. Panorama Commit Dialog



Doing a commit will overwrite the running configuration. Do you want to continue?

Commit Type ○ Panorama ○ Template ● Device Group ○ Collector Group

WARNING: Panorama candidate configuration has not been committed. It is recommended to commit on Panorama before committing to managed devices.

Filters

- □ Commit State
  - □ In Sync (1)
  - □ Out of Sync (10)
- □ Device State
  - □ Connected (11)
- □ Platforms
  - □ PA-200 (1)
  - □ PA-3050 (6)
  - □ PA-4060 (2)
  - □ PA-5050 (2)
- □ Device Groups
  - □ FALCON (2)
  - □ HAWK (2)
  - □ MERLIN (1)
  - □ NOT-OSPREY (3)
  - □ OSPREY (3)

Name	Last Commit State	HA Status	Preview Changes
□ NOT-OSPREY			Preview Changes
□ 3050-w-2		Passive	
□ VR-20	Out of Sync		Preview Changes
□ VWIRE01	Out of Sync		Preview Changes
□ VWIRE02	Out of Sync		Preview Changes
□ OSPREY			Preview Changes
□ 3050-w-1		Active	
□ VR-20	Out of Sync		Preview Changes
□ VWIRE01	Out of Sync		Preview Changes

□ Group HA Peers □ Filter Selected (0)

☑ Merge with Device Candidate Config ☑ Include Device and Network Templates ☑ Force Template Values

The Commit dialog has the following options:

- **Commit Type**:
  - **Panorama**—Commit the current candidate configuration for Panorama.
  - **Template**—Commit template changes from Panorama to the selected firewalls. When committing templates, you can select a subset of firewalls if desired.
  - **Device Group**—Commit firewall configuration changes from Panorama to the selected firewall/virtual system(s).
  - **Collector Group**—Commit changes only to Panorama log Collector Groups. This will commit changes made in the **Panorama > Collector Groups** page and will apply those changes to the Log Collector appliance.
- **Filters**—If the **Commit Type** is **Device Group** or **Template**, you can filter the list of firewalls.
- Firewall name and status—If the **Commit Type** is **Device Group** or **Template**, you can sort the list by device group or template Name, Last Commit State, or HA Status (for firewall peers in a high availability configuration) by clicking the headers of those columns. If the **Commit Type** is **Device Group**, the Name column displays the full tree hierarchy of device groups, including firewall and virtual system (vsys) names.
- **Preview Changes**—If the **Commit Type** is **Panorama**, you can compare the candidate configuration to the running configuration. Use the **Lines of Context** drop-down to specify the number of lines—from the compared configuration files—to display before and after the highlighted differences. If you select **All**, the results include the entire configuration files. Changes are color-coded based on settings that you and other

administrators added (green), modified (yellow), or deleted (red) since the last commit. The **Panorama > Config Audit** feature performs the same function (see “Comparing Configuration Files”).

Because the preview results display in a new window, your browser must allow pop-ups. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-ups.

- **Group HA Peers**—If the **Commit Type** is **Device Group** or **Template**, you can select this check box to display each pair of firewall HA peers as a single entry.
- **Filter Selected**—If the **Commit Type** is **Device Group** or **Template**, you can filter the list to display only specific firewalls by selecting those firewalls and then selecting the **Filter Selected** check box.
- **Merge with Candidate Config**—This option is available if the **Commit Type** is **Device Group** or **Template**. If you select this check box, the firewall includes its local candidate configuration when the commit is invoked from Panorama. If this check box is cleared, the firewall excludes its local candidate configuration. It is important to clear this check box when local administrators are making changes on a firewall and you want to exclude their changes when pushing a configuration from Panorama.
- **Include Device and Network Templates**—This option is available if the **Commit Type** is **Device Group**. The commit will include the device and network settings in the template or template stack to which the selected firewalls are assigned (see “Managing Templates and Template Stacks”). You can also select **Template** as the **Commit Type** to commit templates to firewalls.
- **Force Template Values**—If the **Commit Type** is **Device Group** or **Template**, you can select this check box to remove objects for which an administrator overrode the template in the local configuration of the firewalls or virtual systems (see “Overriding Template Settings”). If the **Commit Type** is **Device Group**, you must select the **Include Device and Network Templates** check box to enable the **Force Template Values** check box.

After the commit is complete, you will see a “Commit succeeded” message. If Panorama generated warnings during the commit, you will see “Commit succeeded with warnings”. To view success or warning message details, in the **Panorama > Managed Devices** page, click the text in the **Last Commit State** column.

Managing Templates and Template Stacks

▶ *Panorama > Templates*

The following topics describe how to manage templates and template stacks:

- “Defining Templates”
- “Defining Template Stacks”
- “Overriding Template Settings”
- “Cloning Templates and Template Stacks”
- “Deleting or Disabling Templates and Template Stacks”

Defining Templates

Through the **Device** and **Network** tabs, templates enable you to deploy a common base configuration to multiple firewalls that require similar settings. 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). Panorama separates the management of these features because firewalls that share policy and object settings do not necessarily have the same device and network settings.

Panorama supports up to 128 templates. You can combine the settings of multiple templates by "Defining Template Stacks".

To create a Panorama template, click **Add** and complete the fields described in the following table. After you add the first template, the **Device** and **Network** tabs display a **Template** drop-down. You can then configure device and network settings for the template selected in the drop-down.

Table 241 Template Settings (Panorama)

Field	Description
Name	Enter a template name (up to 31 characters). Use only letters, numbers, spaces, hyphens, periods, and underscores. The name is case-sensitive and must be unique. In the **Device** and **Network** tabs, this name will appear in the **Template** drop-down. The settings you modify in these tabs apply only to the selected **Template**.
Default VSYS	Select a virtual system (vsys) if you want Panorama to push configurations that are specific to that vsys (for example, interfaces) to firewalls that don't have multiple virtual systems.
Description	Enter a description for the template.
Devices	Select the check box for each firewall that you want to add to the template. If you will use the template only within a stack, do not assign firewalls to the template, just to the stack (see "Defining Template Stacks"). If the list of firewalls is long, you can filter it by **Platforms**, **Device Groups**, **Tags**, and **HA Status**. For each of these categories, the dialog displays the number of managed firewalls. **Note:** *You can assign firewalls that have non-matching modes (VPN mode, multi-vsys mode, or operational mode) to the same template. Panorama pushes mode-specific settings only to firewalls that support those modes. For example, Panorama pushes IPSec tunnels only to firewalls that have VPN mode enabled.*
Group HA Peers	Select the check box to group firewalls that are high availability (HA) peers. 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 option enables you to easily identify firewalls that have an HA configuration. When pushing template settings, you can push to the grouped pair instead of to each firewall individually.
Filter Selected	To display only specific firewalls, select the corresponding firewall check boxes and select the **Filter Selected** check box.

After configuring a template, you must perform a Panorama commit and a template commit to push the configuration changes to the firewalls that are assigned to the template. For details, see "Committing your Changes in Panorama".

Defining Template Stacks

A template stack is a combination of templates. By assigning firewalls to a stack, you can push all the necessary settings to them without the redundancy of adding every setting to every template. Panorama supports up to 128 stacks.

! *Panorama doesn't validate template combinations so avoid ordering templates in a way that creates invalid relationships. For example, if the ethernet1/1 interface is Layer 3 in Template_A but is Layer 2 with a VLAN in Template_B, and Template_A has a higher priority, Panorama will push ethernet1/1 as a Layer 3 type but assigned to a VLAN.*

A template configuration cannot reference a configuration in another template, even if both templates are in the same stack. For example, a zone configuration in Template_A cannot reference a zone protection profile that is defined in Template_B even if Template_A and Template_B are in the same stack.

To create a stack, in the **Panorama > Templates** page, click **Add Stack** and complete the fields described in the following table.

Table 242 Stack Settings (Panorama)

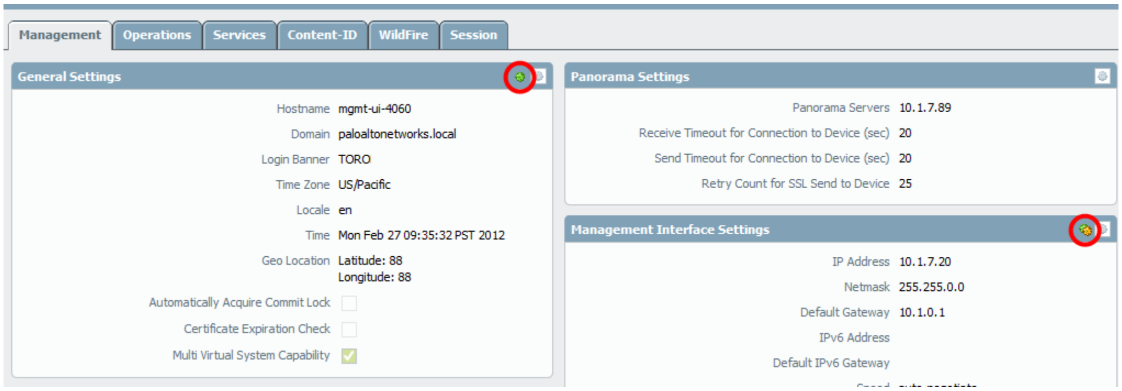
Field	Description
Name	Enter a stack name (up to 31 characters). Use only letters, numbers, and underscores. The initial character must be a letter. The name is case-sensitive and must be unique. In the **Device** and **Network** tabs, the **Template** drop-down will display the stack name and its assigned templates.
Description	Enter a description for the stack.
Templates	For each template you want to include in the stack (up to 16), click **Add** and select the template. If templates have duplicate settings, Panorama pushes only the settings of the higher template in the list to the assigned firewalls. For example, if Template_A is above Template_B in the list, and both templates define the ethernet1/1 interface, Panorama pushes the ethernet1/1 definition from Template_A and not from Template_B. To change the order, select a template and click **Move Up** or **Move Down**.
Devices	Select the check box for each firewall that you want to add to the stack. If the list of firewalls is long, you can filter it by **Platforms**, **Device Groups**, **Tags**, and **HA Status**. **Note:** *You can assign firewalls that have non-matching modes (VPN mode, multi-vsys mode, or operational mode) to the same stack. Panorama pushes mode-specific settings only to firewalls that support those modes. For example, Panorama pushes IPSec tunnels only to firewalls that have VPN mode enabled.*
Group HA Peers	Select the check box to group firewalls that are high availability (HA) peers. This option enables you to easily identify firewalls that have an HA configuration. When pushing settings, you can push to the grouped pair instead of to each firewall individually.
Filter Selected	To display only specific firewalls, select the firewall check boxes and select the **Filter Selected** check box.

Overriding Template Settings

When applying a template or template stack to control device and network settings on a firewall, you can override some settings to use the local firewall configuration. For example, you can deploy a base configuration to a global group of firewalls but use an override to configure specific time zone settings directly on the firewalls.

To identify settings that have templates applied, the web interface displays icons as shown in Figure 17:

Figure 17. Template Indicators



General Settings

Hostname	mgmt-ui-4060
Domain	paloaltonetworks.local
Login Banner	TORO
Time Zone	US/Pacific
Locale	en
Time	Mon Feb 27 09:35:32 PST 2012
Geo Location	Latitude: 88 Longitude: 88
Automatically Acquire Commit Lock	□
Certificate Expiration Check	□
Multi Virtual System Capability	☑

Panorama Settings

Panorama Servers	10.1.7.89
Receive Timeout for Connection to Device (sec)	20
Send Timeout for Connection to Device (sec)	20
Retry Count for SSL Send to Device	25

Management Interface Settings

IP Address	10.1.7.20
Netmask	255.255.0.0
Default Gateway	10.1.0.1
IPv6 Address	
Default IPv6 Gateway	

The green icon 🟩 indicates that Panorama applied a template and the settings have no overrides. The orange-overlapping-green icon 🟧 indicates that Panorama applied a template and some settings have overrides.

To override a device or network setting that Panorama pushes from a template:

1. Switch **Context** to the firewall, or access the firewall web interface directly.
2. Navigate to the setting.
3. If the page displays the setting in a table, select the row for that setting and click the **Override** button. Otherwise, edit the section that displays the setting (as in Figure 17) and click the green icon 🟩 for the setting.
4. Enter the override values and click **OK**.

The firewall copies the setting to its local configuration and the template will no longer control the setting. To revert the change, click the **Restore** button: the firewall will resume inheriting the setting from the template. When doing a commit from Panorama to a managed firewall that contains overrides, you can select the **Force Template Values** check box to have Panorama templates assume control over any overridden objects.

When overriding **Device > High Availability** settings, the overrides are for individual values and parameters inside of configuration trees: the firewall does not apply overrides to an entire tree configuration. This includes items such as DNS servers, Management IP, or NTP server settings. For items such as interfaces and RADIUS server profiles, you apply overrides to the entire object, not internal values.

Cloning Templates and Template Stacks

To clone a template or template stack, select it in the **Panorama > Templates** page and click **Clone**.

Deleting or Disabling Templates and Template Stacks

To delete a template or template stack, select it in the **Panorama > Templates** page and click **Delete**. Deleting a template or template stack, or removing a firewall from one, will not delete the values that Panorama has pushed to the firewall. When you remove a firewall from a template or template stack, Panorama no longer pushes new updates to the firewall.

To disable a template or template stack for a firewall, access the web interface of that firewall, select **Device > Setup > Management**, edit the **Panorama Settings**, and click the **Disable Device and Network Template** button.

Logging and Reporting

Panorama performs two functions: configuration (of firewalls and Panorama itself) and log collection.

To facilitate scalability in large deployments, you can use an M-Series appliance to separate the management and log collection functions on Panorama. An M-Series appliance provides a comprehensive log collection solution for Palo Alto Networks firewalls. This helps offload the traffic intensive log collection process from your Panorama management server; once deployed, you can configure each firewall to send logs to an M-Series appliance configured as a Log Collector. For more information on deploying a distributed log collection architecture, and for configuring and managing the Log Collectors using the Panorama server, refer to the Panorama Administrator's Guide.

The Panorama logs and reports —ACC, AppScope, PDF Reports, and Logs viewer— provide information about user activity in the managed network. To view user/network activity on Panorama, you do not need to configure explicit log forwarding. Log forwarding is required for long term log storage and for generating reports using logs stored locally in Panorama. If log forwarding is enabled, by default logs are buffered on the firewall and sent at a predefined interval to Panorama.

The **ACC** tab in Panorama, by default displays information stored locally on Panorama. You can however, change the data source so that Panorama accesses information from the connected firewalls; all the tables pull information dynamically and display an aggregated view of the traffic on your network.

You can generate and schedule custom reports on Panorama. For scheduled predefined and custom reports, report statistics are aggregated every 15 minutes and are forwarded to Panorama on an hourly basis.

Enable Log Forwarding

▶ ***Panorama > Log Settings***

Use this page to enable log forwarding from Panorama. Panorama can aggregate firewall and Managed Collector logs and forward them to the configured destinations in the form of SNMP traps, syslog messages, and email notifications. If you have not set up server profiles to define the destinations, see "Configuring SNMP Trap Destinations", "Configuring Syslog Servers", and "Configuring Email Notification Settings".

On a Panorama virtual appliance, use the **Panorama > Log Settings** page to enable forwarding of firewall logs, Managed Collector logs, and local Panorama logs. On an M-Series appliance in Panorama mode, use the **Panorama > Log Settings** page to enable forwarding of Managed Collector logs and local Panorama logs, but configure Collector Groups to enable forwarding of firewall logs (see "Defining Log Collector Groups").

The following table describes the logs and forwarding options on the **Panorama > Log Settings** page.

Correlation, HIP Match, Traffic, Threat, and WildFire™ logs apply only to firewalls, and therefore will not appear on this page if you use an M-Series appliance in Panorama mode. The Panorama virtual appliance displays all log types.

Table 243. Log Settings

Section	Description
System	To enable log forwarding for a particular severity level, click the corresponding link in the Severity column and select the desired server profiles. The **Remove all** button enables you to reset your choices to the defaults. The severity indicates the urgency and impact of the system event: • **Critical**—Indicates a failure and the need for immediate attention (for example, hardware failures, including HA failover and link failures). • **High**—Indicates an impending failure or condition that can impair the operational efficiency or security of the firewall (for example, dropped connections with external servers such as LDAP and RADIUS servers). • **Medium**—Indicates a condition that can escalate into a more serious issue, such as a failure to complete an antivirus package upgrade. • **Low**—Indicates something that might be a problem or is likely to become a problem, such as user password changes. • **Informational**—Requires no attention. These logs provide useful information during normal operation of the system. This level covers configuration changes and all other events that other severity levels do not cover.

Table 243. Log Settings (Continued)

Section	Description
Correlation	Correlation logs are created when the definition for a correlation object matches traffic patterns on your network. For information on correlation objects, see "Using the Automated Correlation Engine". Panorama uses the correlation objects to query the aggregated logs (forwarded to it from the managed firewalls and log collectors) for matches and logs the correlation events. These correlation events can be sent as syslog messages, email notifications, or as SNMP traps. To enable log forwarding for a particular severity level, click the corresponding link in the Severity column and select the desired server profiles. The severity indicates the urgency and impact of the match; it broadly assesses the extent of damage or escalation pattern observed, and the frequency of occurrence. Because correlation objects are focused on detecting threats, the correlated events typically relate to identifying compromised hosts on the network and the severity implies the following: • **Critical**—Confirms that a host has been compromised based on correlated events that indicate an escalation pattern. For example, a critical event is logged when a host that received a file with a malicious verdict by WildFire, exhibits the same command-and-control activity that was observed in the WildFire sandbox for that malicious file. • **High**—Indicates that a host is very likely compromised based on a correlation between multiple threat events, such as malware detected anywhere on the network that matches the command-and-control activity being generated from a particular host. • **Medium**—Indicates that a host is likely compromised based on the detection of one or multiple suspicious events, such as repeated visits to known malicious URLs that suggests a scripted command-and-control activity. • **Low**—Indicates that a host is possibly compromised based on the detection of one or multiple suspicious events, such as a visit to a malicious URL or a dynamic DNS domain. • **Informational**—Detects an event that may be useful in aggregate for identifying suspicious activity; each event is not necessarily significant on its own.
Config	Config logs record all changes to the device configuration. To enable forwarding, click the edit icon and select the desired server profiles.
HIP Match	The HIP match log lists the host information profile (HIP) match requests for GlobalProtect™. To enable forwarding, click the edit icon and select the desired server profiles.
Traffic	Traffic logs capture details (for example, origin and destination) of traffic that matches a policy. To enable forwarding, click the edit icon and select the desired server profiles.

Table 243. Log Settings (Continued)

Section	Description
Threat	To enable log forwarding for a particular severity level, click the corresponding link in the Severity column and select the desired server profiles. The severity indicates the urgency and impact of the threat: • **Critical**—Serious threats such as those that affect default installations of widely deployed software, result in root compromise of servers, and the exploit code is widely available to attackers. The attacker usually does not need any special authentication credentials or knowledge about the individual victims and the target does not need to be manipulated into performing any special functions. • **High**—Threats that have the ability to become critical but have mitigating factors; for example, they may be difficult to exploit, do not result in elevated privileges, or do not have a large victim pool. • **Medium**—Minor threats in which impact is minimized, such as DoS attacks that do not compromise the target or exploits that require an attacker to reside on the same LAN as the victim, affect only non-standard configurations or obscure applications, or provide very limited access. In addition, WildFire log entries with a malware verdict are logged as Medium. • **Low**—Warning-level threats that have very little impact on the infrastructure of an organization. They usually require local or physical system access and can often result in victim privacy or DoS issues and information leakage. Data Filtering profile matches are logged as Low. • **Informational**—Suspicious events that do not pose an immediate threat, but that are reported to call attention to deeper problems that could possibly exist. Some examples of information logs are: URL Filtering log entries, WildFire log entries with a benign verdict, or Data Filtering logs.
WildFire	WildFire scans files and assigns a verdict. To enable log forwarding for a particular verdict, click the corresponding link in the Verdict column and select the desired server profiles. The verdicts are: • **benign**—Indicates that the file is safe. • **grayware**—Indicates that the file has suspicious qualities or behavior but is not malicious. • **malicious**—Indicates that the file contains malicious code.

Managing Log Collectors

▶ *Panorama > Managed Collectors*

Use the Managed Collectors page to configure, manage, and update Log Collector devices.

- To add a Log Collector, see "Adding a Log Collector"
- To install a software update, see "Installing a Software Update on a Log Collector"

Adding a Log Collector

To add a Log Collector, click **Add** and complete the following fields

Table 244. Managed Collectors Page

Field	Description
General Tab	
Collector S/N	Enter the serial number of the Log Collector device.
Collector Name	Enter a name to identify this Log Collector (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. This name displays as the hostname of the Log Collector.
Device Log Collection	Select the interface to use for firewall log collection. By default, the management interface (MGT) performs this function. To select Eth1 or Eth2, you must first enable and configure those interfaces (**Panorama > Setup**, Eth1/Eth2 Interface Settings).
Collector Group Communication	Select the interface to use for communication within Collector Groups. By default, the management interface (MGT) performs this function. To select Eth1 or Eth2, you must first enable and configure those interfaces (**Panorama > Setup**, Eth1/Eth2 Interface Settings).
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 “Managing Device Certificates”). When you assign a Syslog server profile to the Collector Group that includes this Log Collector, the **Transport** protocol of the server profile must be **SSL** (see “Configuring Syslog Servers”).
Panorama Server IP	Specify the IP address of the Panorama server used to manage this collector.
Panorama Server IP 2	Specify the IP address of the secondary device if the Panorama management server is in HA mode.
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 server).
Secondary DNS Server	Enter the IP address a secondary DNS server to use if the primary server is unavailable (optional).
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	Enter the IP address or host name of secondary NTP servers to use if the primary server is unavailable (optional).
Timezone	Select the time zone of the Log Collector.
Latitude	Enter the latitude (-90.0 to 90.0) of the Log Collector that is used in the traffic and threat maps for App Scope.
Longitude	Enter the longitude (-180.0 to 180.0) of the Log Collector that is used in the traffic and threat maps for App-Scope.
Authentication Tab	

Table 244. Managed Collectors Page

Field	Description
Users	This field will always show **admin** and is used for the local CLI login name on the Log Collector.
Mode	Select **Password** to manually enter a password to be used for authentication, or select **Password Hash** to enter a hash value. To create a password hash from the Panorama management server CLI, run the following: `request password-hash password password123` This will return a hash value for the password *password123 (Example-$1$urlishri$aLP2by.u2A1IQ/Njh5TFy9).* Copy the hash value from the CLI and paste to the **Password Hash** field. When you commit your changes, the new hash will be pushed to the Log Collector and the new local admin login password will be *password123*.
Failed Attempts	Specify the number of failed login attempts (1-10) that are allowed for the web interface and CLI before the account is locked. The default 0 means there is no limit.
Lockout Time (min)	Specify the number of minutes that a user is locked out (0-60 minutes) if the number of failed attempts is reached. The default 0 means that there is no limit to the number of attempts.
Management Tab This tab only applies to the M-Series appliance, not the Panorama virtual appliance. By default, the M-Series appliance uses the management (MGT) port for configuration, log collection, and Collector Group communication. However, if you configure Eth1 or Eth2 for log collection and/or Collector Group communication, it is a best practice to define a separate subnet for the MGT interface that is more private than the Eth1 or Eth2 subnets. You define the subnet in the **Netmask** (for IPv4) or **IPv6 Address** (define a prefix) field. **Note:** *To complete the configuration of the management interface, you must specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway. If you commit a partial configuration (for example, you might omit the default gateway), you can only access the M-Series appliance via the console port for future configuration changes. It is recommended that you commit a complete configuration.*	
Speed and Duplex	Select the interface speed in Mbps (10, 100, or 1000) and the interface transmission mode full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
IP Address	If your network uses IPv4, assign an IPv4 address (default 192.168.1.1) to the management port of the Log Collector.
Netmask	If you assigned an IPv4 address to the management port, enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to the management port, assign an IPv4 address to the default router (it must be on the same subnet as the management port).
IPv6 Address	If your network uses IPv6, assign an IPv6 address to the management port of the Log Collector. To indicate the netmask, enter an IPv6 prefix length (for example, 2001:400:f00::1/64).
IPv6 Default Gateway	If you assigned an IPv6 address to the management port, assign an IPv6 address to the default router (it must be on the same subnet as the management port).

Table 244. Managed Collectors Page

Field	Description
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range 576-1500, default 1500).
Management Interface Services	Select the services you want enabled on the management interface of the Log Collector device: • SSH • Ping • SNMP (Simple Network Managed Protocol)
Permitted IP Addresses	Click **Add** to enter the list of IP addresses from which management is allowed for this interface.
Eth1 Tab This tab only applies to the M-Series appliance, not the Panorama virtual appliance. The tab is only available if you configured Eth1 in the Panorama management settings (**Panorama > Setup > Management**, Eth1 Interface Settings). **Note:** *You cannot commit the Eth1 configuration unless you specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway.*	
Eth1	Select the check box to enable this interface.
Speed and Duplex	Select the interface speed in Mbps (10, 100, or 1000) and the interface transmission mode full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
IP Address	If your network uses IPv4, assign an IPv4 address to Eth1.
Netmask	If you assigned an IPv4 address to Eth1, enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to Eth1, assign an IPv4 address to the default router (it must be on the same subnet as Eth1).
IPv6 Address	If your network uses IPv6, assign an IPv6 address to Eth1. To indicate the netmask, enter an IPv6 prefix length (for example, 2001:400:f00::1/64).
IPv6 Default Gateway	If you assigned an IPv6 address to Eth1, assign an the IPv6 address to the default router (it must be on the same subnet as Eth1).
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range 576-1500, default 1500).
Ping	Select the check box if you want to enable Ping on the Eth1 interface.
Permitted IP Addresses	Click **Add** to enter the list of IP addresses from which management is allowed for this interface.
Eth2 Tab This tab only applies to the M-Series appliance, not the Panorama virtual appliance. The tab is only available if you configured Eth2 in the Panorama management settings (**Panorama > Setup > Management**, Eth2 Interface Settings). **Note:** *You cannot commit the Eth2 configuration unless you specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway.*	
Eth2	Select the check box to enable this interface.
Speed and Duplex	Select the interface speed in Mbps (10, 100, or 1000) and the interface transmission mode full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).

Table 244. Managed Collectors Page

Field	Description
IP Address	If your network uses IPv4, assign an IPv4 address to Eth2.
Netmask	If you assigned an IPv4 address to Eth2, enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to Eth2, assign an IPv4 address to the default router (it must be on the same subnet as Eth2).
IPv6 Address	If your network uses IPv6, assign an IPv6 address to Eth2. To indicate the netmask, enter an IPv6 prefix length (for example, 2001:400:f00::1/64).
IPv6 Default Gateway	If you assigned an IPv6 address to Eth2, assign an the IPv6 address to the default router (it must be on the same subnet Eth2).
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range 576-1500, default 1500).
Ping	Select the check box if you want to enable Ping on the Eth2 interface.
Permitted IP Addresses	Click **Add** to enter the list of IP addresses from which management is allowed for this interface.
Disks Tab Click **Add** to select the RAID 1 disk pair that the Log Collector will use to store logs. You can add additional disk pairs as needed to expand the storage capacity. To make an added disk pair available to the Log Collector, select the check box. To make all the added disk pairs available, select the **Enable Disk Pair** check box. By default, the M-Series appliance is shipped with the first RAID 1 pair enabled and installed in bays A1/A2. To increase storage capacity, you can add up to three more RAID 1 pairs in bays B1/B2, C1/C2, and D1/D2. In the software, the RAID 1 pair in bays A1/A2 is named **Disk Pair A**. After you enable new 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 logging rate is reduced. In the **Panorama > Managed Collectors** page, the Redistribution State column indicates the completion status of the process as a percentage.	

After adding Log Collectors, you can click the **Statistics** link for each collector to open the Collector Statistics window, which shows disk information, performance numbers for the CPU, and the average log rate (logs/second). For a better understanding of the log range you are reviewing, you can also view information on the oldest log that the collector received.

Installing a Software Update on a Log Collector

To install a software image on the Log Collector (an M-Series appliance in Log Collector mode), download or upload the image to Panorama (see "Managing Device Updates and Licenses"), then click **Install** in the **Panorama > Managed Collectors** page and complete the following details:

Table 245 Software Update on a Log Collector

Field	Description
File	Select a software image file. You must have either downloaded or uploaded the file using the **Panorama > Device Deployment > Software** page.
Devices	Select the Log Collectors on which you want to install the image.
Upload only to device (do not Install)	Select this option if you want to upload the image to the Log Collector, but do not want to reboot it now. Until you initiate a reboot, the software image is not installed.
Reboot device after Install	Select this option if you want to upload and install the software image. The installation process triggers a reboot.

Defining Log Collector Groups

▶ *Panorama > Collector Groups*

In Collector Groups, you assign managed firewalls to Log Collectors. After you establish the Log Collectors and configure the firewalls, PAN-OS sends the firewall logs to the Log Collectors. Panorama then queries the Log Collectors for aggregated log viewing or investigation.

To configure Collector Groups, click **Add** and complete the following parameters:

Table 246. Collector Groups Settings

Field	Description
General Tab	
Name	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 current storage quota for firewall logs that the Collector Group receives. Clicking the capacity text opens the **Log Storage Settings** dialog, where you can set the storage **Quota** and expiration period (**Max Days**) for each log type, log summary type, and extended threat PCAPs. For details on quotas and expiration periods, see the Logging and Reporting Settings under "Defining Management Settings". You can also click **Restore Defaults** to use the default settings.

Table 246. Collector Groups Settings (Continued)

Field	Description
Min Retention Period (days)	Specify the minimum log retention period (1-2000 days) that Panorama maintains across all Log Collectors in the Collector Group before generating an alert. Panorama generates an alert violation in the form of a system log if the current date minus the date of the oldest log is less than the defined minimum retention period.
Enable log redundancy across collectors	If you select this check box, 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. After you enable redundancy, Panorama redistributes the 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 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 platform (all M-100 appliances or all M-500 appliances). **Note:** *Because enabling redundancy creates more logs, this configuration requires more storage capacity. When a Collector Group runs out of space, it deletes older logs. 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.*

Table 246. Collector Groups Settings (Continued)

Field	Description
Monitoring Tab	
SNMP	The SNMP option enables you to collect information about the Log Collectors, including: connection status, Disk drive statistics, software version, average CPU, Average log/second, and storage duration per DB type (e.g. minutes, hours, days, weeks). SNMP information is available on a per Collector Group basis. Specify the SNMP settings: • Location—Specify the location of the Log Collector device. • Contact—Specify an email contact for this collector. • Access Setting—Specify the SNMP version that will be used to communicate with the Panorama management server (V2c or V3). If you select V3, specify the following: – Views— Click Add and configure the following settings: › View**—**Specify a name for a view. › OID—Specify the object identifier (OID). › Option (include or exclude)—Choose whether the OID is to be included or excluded from the view. › Mask—Specify a mask value for a filter on the OID in hexadecimal format (for example, 0xf0) – Users—Click **Add** and configure the following settings: › Users—Specify a user name that will be used for authentication between the Log Collector and SNMP management server. › View**—**Specify the group of views for the user. › Authpwd**—**Specify the user's authentication password (minimum 8 characters). Only Secure Hash Algorithm (SHA) is supported. › Privpwd**—**Specify the user's encryption password (minimum 8 characters). Only Advanced Encryption Standard (AES) is supported. • SNMP Community—Specify the SNMP community string that is used by your SNMP management environment. SNMPv2c Only (default is public).
Device Log Forwarding Tab	
Collector Group Members	Click **Add** and, from the drop-down, select the Log Collectors (up to eight) that will be part of this group. The drop-down will show all Log Collectors that are available in the **Panorama > Managed Collectors** page. 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 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 platform (all M-100 appliances or all M-500 appliances).

Table 246. Collector Groups Settings (Continued)

Field	Description
Devices	You must add Collector Group Members before you can add firewalls to the Collector Group. To add firewalls, click **Add**, click **Modify** in the Devices list, select the managed firewalls, then click **OK**. To assign the firewalls to Log Collectors for log forwarding, click **Add** in the Collectors list, and select the Log Collectors. The first Log Collector you specify will be the primary Log Collector for the firewalls. If the primary Log Collector fails, the firewalls will send logs to the secondary Log Collector. If the secondary fails, the firewalls will send logs to the tertiary Log Collector, and so on. To change the order, select a Log Collector and click the **Move Up** or **Move Down** buttons. After you assign all the Log Collectors in the desired order, click **OK**.
Collector Log Forwarding Tab	
System	For all managed firewalls that are forwarding logs to this Collector Group, select the logs and events by Severity that you want to aggregate and forward to SNMP Trap, Email, and Syslog servers. If you have not already configured the server profiles for the destinations, see“Configuring SNMP Trap Destinations”, “Configuring Syslog Servers”, and “Configuring Email Notification Settings”.
Config	
HIP Match	
Traffic	
Threat	
WildFire	
Correlation	

Generating User Activity Reports

▶ *Monitor > PDF Reports > User Activity Report*

The Panorama user activity report summarizes user activity across all of the managed firewalls. It is based on firewall data that has been forwarded to Panorama. Refer to “Managing User/Group Activity Reports” for general information on creating user activity reports.

Managing Device Updates and Licenses

▶ *Panorama > Device Deployment*

The **Device Deployment** pages display current deployment information for the managed firewalls. They also enable you to manage software and content updates, manage licenses, and schedule updates on the managed firewalls and Log Collectors.

Table 247. Panorama Device Deployment Tabs

Page	Description
Device Deployment > Software	Lists the software updates that are available for installation on the managed firewalls and Log Collectors.
Device Deployment > SSL VPN Client	Lists the SSL VPN client software updates that are available for installation on the managed firewalls.
Device Deployment > GlobalProtect Client	Lists the GlobalProtect client software updates that are available for installation on the managed firewalls.
Device Deployment > Dynamic Updates	Lists the dynamic content updates that are available for deployment on the managed firewalls and Log Collectors. Palo Alto Networks periodically posts updates with new or revised application and threat definitions, antivirus signatures, URL filtering categories, GlobalProtect data, and WildFire signatures. To receive the updates, corresponding subscriptions are required. To automate the process of downloading and installing dynamic updates, see “Scheduling Dynamic Updates”.

Table 247. Panorama Device Deployment Tabs

Page	Description
Device Deployment > Licenses	Lists each managed firewall and the current license status. Each entry indicates whether the license is active (✓ icon) or inactive (✗ icon), along with the expiration date for active licenses. 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. Perform any of the following actions on this page: • Click **Refresh** to manually update the licenses of firewalls that don't have direct Internet access. • Click **Activate** to activate a license. Select the managed firewalls for activation and enter the authentication code that Palo Alto Networks provided for the firewall. • Click **Deactivate VMs** to deactivate all the licenses and subscriptions/ entitlements installed on a VM-Series firewall. Select the VM-Series firewalls from which to deactivate licenses; firewall running versions earlier than PAN-OS 7.0 are not displayed. – Click **Continue** to deactivate the licenses and automatically register the changes with the licensing server. The licenses are credited back to your account and are available for reuse. – Click **Complete Manually** to generate a token file. Use this option if your Panorama does not have direct Internet access. To complete the deactivation process, you must log into the Support portal and upload the token file that was generated. On completing the deactivation process, the licenses are credited back to your account and are available for reuse.

Perform any of the following actions on the **Software**, **SSL VPN Client**, **GlobalProtect Client**, or **Dynamic Updates** pages:

- Click **Check Now** to view the latest information on updates from Palo Alto Networks.
- Click **Release Notes** to view a description of the changes in a release (this is not available for uploaded software).
- Click **Download** to download a new release from the Palo Alto Networks Update Server. When the download is complete, the **Available** column displays Downloaded. The steps to then install or activate the update depend on the type:
  - PAN-OS **Software—**Click **Install** in the Action column and select the firewalls. If you select the **Reboot device after install** check box, the firewalls will reboot during installation. The installation cannot finish until the firewalls reboot. If you select the **Upload only to device (do not install)** check box, PAN-OS doesn't install the uploaded image until you log in to the firewall, select **Device > Software**, and click **Install** in the Action column.
  - **SSL VPN Client** or **GlobalProtect Client** software—Click **Activate** in the Action column and select the firewalls.
  - Dynamic Updates—Click **Install** in the Action column and select the firewalls.

- Click **Upload** to upload an update to Panorama from another computer. You must have already downloaded the update to that computer from the Software Update site. When the upload is complete, the **Available** column displays Uploaded. The steps to then install or activate the update depend on the type:
  - PAN-OS **Software**—Click **Install** in the Action column and select the firewalls. If you select the **Reboot device after install** check box, the firewall will reboot during installation. The installation cannot finish until the device reboots. If you select the **Upload only to device (do not install)** check box, PAN-OS doesn't install the uploaded image until you log in to the firewall, select **Device > Software**, and click **Install** in the Action column.
  - **SSL VPN Client** or **GlobalProtect Client** software—Click **Activate From File**, select the **File Name** you just uploaded, and select the firewalls.
  - **Dynamic Updates**—Click **Install From File**, select the content **Type**, select the **File Name** you just uploaded, and select the firewalls.
- Click the Delete icon ☒ to delete an outdated release that you downloaded or uploaded.

Scheduling Dynamic Updates

▶ *Panorama > Device Deployment > Dynamic Updates*

Click the **Schedules** link to schedule automatic updates for managed firewalls and managed Log Collectors. Specify the frequency and timing for the updates and whether to download and install the update or to only download the updates.

To create a schedule, click **Add** and fill in the following details:

Table 248. Scheduling Dynamic Updates

Field	Description
Name	Enter a name to identify the scheduled job (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.
Disabled	Select the check box to disable the scheduled job.
Type	Select the dynamic update type that you would like to schedule (App and threat, antivirus, WildFire, URL Database).
Action	**Download Only**: The scheduled update is downloaded to the selected firewalls/Log Collectors. Then, at your convenience, you can install the downloaded update by clicking the **Install** link in the Action column on the Dynamic Updates page. **Download and Install**: The scheduled update is download and installed; a reboot is initiated on each firewall/Log Collector to complete the installation.
Recurrence	Select the interval at which Panorama checks in with the update server. The recurrence options vary by type of update.
Time	For a **Daily** update, select the **Time** from the 24-hr clock. For a **Weekly** update, select the **Day** of week, and the **Time** from the 24-hr clock.
Eligible devices	Use the filters to select the firewalls/Log Collectors for which you wish to schedule dynamic updates.

Scheduling Configuration Exports

▶ *Panorama > Scheduled Config Export*

Panorama saves a backup of running configurations from all managed firewalls in addition to its own running configuration. Use the **Scheduled Config Export** page to collect the running configurations from Panorama and all the managed firewalls, package them in one gzip file, and schedule the package for daily delivery to an FTP server or by using Secure Copy (SCP) to transfer data securely to a remote host. The files are in XML format with file names that are based on the firewall serial numbers.

If Panorama has a high availability (HA) configuration, you must schedule configuration exports on each peer to ensure the exports continue after a failover. Panorama does not synchronize scheduled configuration exports between HA peers.

Table 249. Scheduling Configuration Bundle Exports

Field	Description
Name	Enter a name to identify the configuration bundle 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 the check box to enable the export job.

Table 249. Scheduling Configuration Bundle Exports (Continued)

Field	Description
Log Type	Select the log type that you would like to export (traffic, threat, URL, data, hipmatch).
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 the firewall to a remote host. You can use SCP to export logs securely, or you can use FTP, which is not a secure protocol.
Hostname	Enter the IP address or host name of the target FTP server.
Port	Enter the port number on the target server.
Path	Specify the path to the folder or directory on the FTP or SCP server where the exported information will be saved. If the configuration bundle is stored in a folder called exported_config within a top level folder Panorama: The syntax for the SCP server path is: **/Panorama/exported_config** The syntax for the FTP server path is: **//Panorama/exported_config**
Enable FTP Passive Mode	Select the check box to use FTP passive mode.
Username	Specify the user name on the target system.
Password Confirm Password	Specify the password for the user on the target system.
Test SCP server connection	Click this button 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.

Upgrading the Panorama Software

▶ *Panorama > Software*

When upgrading to a new Panorama software version, you can use the **Panorama > Software** page to view the latest versions available from Palo Alto Networks, read the associated release notes, and select a version to download and install (a support license is required). If Panorama does not have access to the external network, you can upload the release image from another computer.

If you will upgrade the Panorama virtual appliance to a 64-bit Panorama version (Panorama 5.1 or later), refer to the Release Notes for recommendations on minimum system requirements and instructions on modifying the virtual machine settings after the upgrade.

By default, the Panorama management server saves up to five versions of software. To make space for newer version downloads, the server automatically deletes the oldest version. You can change the number of software images that Panorama saves and manually delete images to free up space.

To upgrade to a new release:

1. Perform one of the following steps to view the latest software releases available from Palo Alto Networks:

   – If Panorama has access to the external network—In the **Panorama > Software** page, click **Check Now**.

   – If Panorama does not have access to the external network—On a computer that can access the external network, use a browser to visit the Software Update site.

2. Perform one of the following steps to access the release notes for the desired software version and review the release changes, fixes, known issues, compatibility issues, and changes in default behavior:

   – If Panorama has access to the external network—In the **Panorama > Software** page, click the Release Notes link for the version.

   – If Panorama does not have access to the external network—In the Software Update site, click the link in the Release Notes column for the desired release.

3. Perform one of the following steps to import the software image into Panorama:

   – If Panorama has access to the external network—In the **Panorama > Software** page, click **Download** in the Action column for the desired release. When the download is complete, the **Available** column displays Downloaded.

   – If Panorama does not have access to the external network:

     i. In the Software Update site, click the link in the Download column for the desired release, then download the software image to a computer that Panorama can access.

     ii. In the **Panorama > Software** page, click the **Upload** button, **Browse** to the software image, then click **OK**. When the upload is complete, the **Available** column displays Uploaded.

4. In the **Panorama > Software** page, click **Install** in the Action column for the release you just downloaded or uploaded. When the installation is complete, you will be logged out while the Panorama system reboots.

Panorama periodically performs a file system integrity check (FSCK) to prevent corruption of the Panorama system files. This check occurs after 8 reboots or at a reboot that occurs 90 days after the last FSCK that Panorama ran. If Panorama is running a FSCK, a warning appears in the web interface and SSH login screens, indicating that an FSCK is in progress and you cannot log in until it completes. The time to complete this process varies by the size of the storage system; depending on the size, it can take several hours before you can log back into Panorama. To view progress, set up console access to Panorama.

To remove the software image of an outdated release from Panorama, click ☒ for that release in the **Panorama > Software** page.

Register VM-Series Firewall as a Service on the NSX Manager

▶ *Panorama > VMware Service Manager*

To automate the provisioning of the VM-Series firewall, use the settings in this section to 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 new VM-Series firewall(s) on each ESX(i) host in the cluster.

If you use Dynamic Address Groups, this feature allows you to secure the virtual network with minimal administrative overhead. As new virtual machines are provisioned or existing machines are modified, the changes in the virtual network are automatically provided as updates to Panorama and are then pushed from Panorama to the managed firewalls. All policy rules that reference these objects (through Dynamic Address Groups) are updated to reflect the changes in the virtual environment and ensures that security policies are consistently applied to all network resources.

Table 250. Configure the VMware Service Manager

Field	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 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 can 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 itself and establish communication with the NSX Manager.
NSX Manager Password	
Confirm NSX Manager Password	
VM-Series OVF URL	Enter the URL (IP address or host name and path) where the NSX Manager can access the file (.ovf) to provision new VM-Series firewalls.
Authorization Code	On the purchase of the VM-Series firewall you received an order fulfillment email. Enter the authorization code provided in the order-fulfillment email.
Template	(Optional) Select the template or template stack to which these VM-Series firewalls will be assigned. For details, see “Managing Templates and Template Stacks”.
Device Group	Select the device group to which these VM-Series firewalls will be assigned. For details, see “Defining Device Groups”.
Notify Device Groups	Select the device group(s) that must be notified of additions or modifications to the virtual machines deployed on the network. When configured, Panorama populates and updates changes to the registered IP addresses to the firewalls in the specified device group(s). 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 needs to 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.

Table 250. Configure the VMware Service Manager (Continued)

Field	Description
Status	Displays the connection status between Panorama and the NSX Manager. When the connection is successful, the status displays as: • Registered: Panorama and the NSX Manager are in sync and the VM-Series firewall is registered as a service on the NSX Manager. The unsuccessful status messages are: • Not connected: Unable to reach/establish a network connection to the NSX Manager. • Not authorized: The access credentials (username and/or password) are incorrect. • Not registered: The service, service manager, or service profile is unavailable or was deleted on the NSX Manager. • Out of sync: The configuration settings defined on Panorama is different from what is defined on the NSX Manager. • No service/ No service profile: Indicates an incomplete configuration on the NSX Manager.
Last Dynamic Update	Displays the date and time when Panorama retrieved the dynamic address group information from the NSX Manager.

Updating Information from the VMware Service Manager

The following actions can be performed on Panorama:

- **Synchronize Dynamic Objects—**Initiates a refresh of the dynamic object information from the NSX Manager. Synchronizing dynamic objects gives you the ability to maintain context on changes in the virtualized environment, and it allows you to safely enable applications by automatically updating the object references in policy.

Note: *On Panorama, you can only view 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 firewall(s). If you are using the VM-Monitoring feature or using the XML API to register IP addresses dynamically to the firewall(s), you must log into each firewall to view the complete list of dynamic addresses that are pushed from Panorama and are locally registered to the firewall.*

- **Remove VMware Service Manager—**Deletes the configuration on how to access the NSX Manager and establish communication between Panorama and the NSX Manager.

Appendix A
COMMON CRITERIA/FEDERAL INFORMATION PROCESSING STANDARDS SUPPORT

You can configure the firewall to support the Common Criteria and the Federal Information Processing Standards 140-2 (FIPS 140-2), which are security certifications that ensure a standard set of security assurances and functionalities. These certifications are often required by civilian U.S. government agencies and government contractors.

Enabling CC/FIPS Mode

Use the following procedure to enable CC/FIPS mode on a software version that supports CC/FIPS. Keep in mind that when you enable CC/FIPS, the device will be reset the factory default settings; all configuration will be removed.

1. Boot the firewall into maintenance mode as follows:

   a. Establish a serial connection to the console port on the firewall.

   b. Enter the following CLI command:
   `debug system maintenance-mode`
   Note: You can also reboot the firewall and type `maint` at the maintenance mode prompt.

   c. The firewall will boot into maintenance mode. Press enter to continue.

2. Select **Set CCEAL4 Mode** from the menu.

3. Select **Enable CCEAL4 Mode** from the menu.

4. When prompted, select **Reboot**.

   After successfully switching to CC/FIPS mode, the following status displays: **`CCEAL4 mode enabled successfully`**. In addition, **`CC`** will display at all times in the status bar at the bottom of the web interface. In addition, the console port will now be available as a status output port only. In addition, the default admin login credentials change to admin/paloalto.

CC/FIPS Security Functions

When CC/FIPS is enabled, the following apply:

- To log into the firewall, the browser must be TLS 1.0 compatible.
- All passwords on the firewall must be at least six characters.
- Accounts are locked after the number of failed attempts that is configured on the **Device > Setup > Management** page. If the firewall is not in CC/FIPS mode, it can be configured so that it never locks out; however in CC/FIPS mode, and lockout time is required.

- The firewall automatically determines the appropriate level of self-testing and enforces the appropriate level of strength in encryption algorithms and cipher suites.
- Non-CC/FIPS approved algorithms are not decrypted and are thus ignored during decryption.
- When configuring IPSec, a subset of the normally available cipher suites is available.
- Self-generated and imported certificates must contain public keys that are 2048 bits (or more).
- The serial port is disabled.
- Telnet, TFTP, and HTTP management connections are unavailable.
- Surf control is not supported.
- High availability (HA) encryption is required.
- PAP authentication is disabled.

Index