

paloalto
NETWORKS®

PAN-OS® Web Interface Reference Guide

Version 7.1

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About this Guide

This guide describes the Palo Alto Networks next-generation firewall and Panorama web interfaces. It provides reference information on how to populate fields within these web interface. For additional information, refer to the following resources:

- 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, 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 release notes, see <https://www.paloaltonetworks.com/documentation/71/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

© 2016-2017 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

Revision Date: December 27, 2017



Table of Contents

Web Interface Basics	11
Firewall Overview	12
Features and Benefits	13
Management Interfaces	14
Last Login Time and Failed Login Attempts	15
Message of the Day	16
Task Manager	17
Language	18
Alarms	19
Commit Changes	20
Lock Configurations	22
Save Candidate Configurations	23
 Dashboard	 25
 ACC	 27
A First Glance at the ACC	28
ACC Views	29
ACC Widgets	29
ACC Actions	31
 Monitor	 35
Monitor > Logs	36
Log Types	36
Log Actions	39
AutoFocus Threat Data for Log Artifacts	40
Monitor > Automated Correlation Engine	42
Monitor > Automated Correlation Engine > Correlation Objects	42
Monitor > Automated Correlation Engine > Correlated Events	43
Monitor > Packet Capture	45
Packet Capture Overview	45
Building Blocks for a Custom Packet Capture	46
Enable Threat Packet Capture	48
Monitor > App Scope	49
App Scope Overview	49
App Scope Summary Report	50
App Scope Change Monitor Report	51
App Scope Change Monitor Options	51
App Scope Threat Monitor Report	52
App Scope Threat Monitor Report Options	53

App Scope Threat Map Report.....	54
App Scope Threat Map Report Options.....	54
App Scope Network Monitor Report	55
App Scope Network Monitor Report Options.....	56
App Scope Traffic Map Report.....	57
App Scope Traffic Map Report Options	57
Monitor > Session Browser	58
Monitor > Botnet.....	59
Managing Botnet Reports	59
Configuring the Botnet Report.....	59
Monitor > PDF Reports.....	61
Monitor > PDF Reports > Manage PDF Summary	61
Monitor > PDF Reports > User Activity Report.....	63
Monitor > PDF Reports > SaaS Application Usage.....	64
Monitor > PDF Reports > Report Groups.....	65
Monitor > PDF Reports > Email Scheduler.....	66
Monitor > Manage Custom Reports	67
Monitor > Reports	68
Policies	69
Policy Types	70
Move or Clone a Policy Rule	71
Policies > Security	72
Security Policy Overview	72
Building Blocks in a Security Policy.....	73
Creating and Managing Policies.....	80
Overriding or Reverting a Security Policy Rule	82
Policies > NAT	84
NAT General Tab	84
NAT Original Packet Tab.....	85
NAT Translated Packet Tab	86
NAT Active/Active HA Binding Tab	87
Policies > QoS.....	89
Policies > Policy Based Forwarding.....	93
Policy Based Forwarding General Tab	93
Policy Based Forwarding Source Tab	94
Policy Based Forwarding Destination/Application/Service Tab.....	95
Policy Based Forwarding Forwarding Tab	95
Policies > Decryption.....	97
Decryption General Tab	97
Decryption Source Tab	98
Decryption Destination Tab	99
Decryption Service/URL Category Tab.....	100
Decryption Options Tab	100
Policies > Application Override	101
Application Override General Tab	101
Application Override Source Tab.....	102

Table of Contents

Application Override Destination Tab	102
Application Override Protocol/Application Tab	103
Policies > Captive Portal.....	104
Captive Portal General Tab	104
Captive Portal Source Tab	105
Captive Portal Destination Tab	105
Captive Portal Service/URL Category Tab.....	106
Captive Portal Action Tab.....	106
Policies > DoS Protection.....	107
DoS Protection General Tab	107
DoS Protection Source Tab	108
DoS Protection Destination Tab	109
DoS Protection Option/Protection Tab.....	109
Objects	111
Move, Clone, Override, or Revert Objects	112
Move or Clone an Object	112
Override or Revert an Object.....	112
Actions in Security Profiles and Custom Objects.....	114
Objects > Addresses	116
Objects > Address Groups.....	118
Objects > Regions	120
Objects > Applications	121
Applications Overview	121
Actions Supported on Applications.....	125
Defining Applications	127
Objects > Application Groups	130
Objects > Application Filters	131
Objects > Services.....	132
Objects > Service Groups.....	133
Objects > Tags	134
Create Tags.....	134
Use the Tag Browser.....	135
Manage Tags.....	136
Objects > External Dynamic Lists.....	138
Objects > Custom Objects.....	140
Objects > Custom Objects > Data Patterns.....	140
Objects > Custom Objects > Spyware/Vulnerability	143
Objects > Custom Objects > URL Category	147
Objects > Security Profiles.....	148
Objects > Security Profiles > Antivirus.....	149
Objects > Security Profiles > Anti-Spyware Profile	151
Objects > Security Profiles > Vulnerability Protection	155
Objects > Security Profiles > URL Filtering	158
Objects > Security Profiles > File Blocking	163
Objects > Security Profiles > WildFire Analysis	164

Objects > Security Profiles > Data Filtering	165
Objects > Security Profiles > DoS Protection	167
Objects > Security Profile Groups	169
Objects > Log Forwarding	170
Objects > Decryption Profile	172
Decryption Profile General Settings	172
Settings to Control Decrypted SSL Traffic	173
Settings to Control Traffic that is not Decrypted	175
Settings to Control Decrypted SSH Traffic	175
Objects > Schedules	176
Network	177
Network > Virtual Wires	178
Network > Interfaces	179
Firewall Interfaces Overview	180
Common Building Blocks for Firewall Interfaces	180
Common Building Blocks for PA-7000 Series Firewall Interfaces	182
Layer 2 Interface	183
Layer 2 Subinterface	184
Layer 3 Interface	185
Layer 3 Subinterface	192
Virtual Wire Interface	198
Virtual Wire Subinterface	199
Tap Interface	200
Log Card Interface	201
Log Card Subinterface	202
Decrypt Mirror Interface	203
Aggregate Ethernet (AE) Interface Group	204
Aggregate Ethernet (AE) Interface	207
HA Interface	208
Network > Interfaces > VLAN	209
Network > Interfaces > Loopback	214
Network > Interfaces > Tunnel	216
Network > Virtual Routers	218
General Settings of a Virtual Router	219
Static Routes	219
Route Redistribution	221
RIP	222
OSPF	225
OSPFv3	230
BGP	236
IP Multicast	244
ECMP	248
More Runtime Stats for a Virtual Router	250
Network > Zones	257
Security Zone Overview	257
Building Blocks of Security Zones	257
Network > VLANs	260

Table of Contents

Network > IPSec Tunnels.....	261
IPSec VPN Tunnel Management.....	261
IPSec Tunnel General Tab.....	262
IPSec Tunnel Proxy IDs Tab.....	264
IPSec Tunnel Status on the Firewall	265
IPSec Tunnel Restart or Refresh	265
Network > DHCP	266
DHCP Overview.....	266
DHCP Addressing	267
DHCP Server.....	267
DHCP Relay	270
DHCP Client	270
Network > DNS Proxy	271
DNS Proxy Overview	271
DNS Proxy Settings	272
Additional DNS Proxy Actions	273
Network > QoS	274
QoS Interface Settings	274
QoS Interface Statistics.....	276
Network > LLDP	277
LLDP Overview	277
Building Blocks of LLDP	278
Network > Network Profiles	281
Network > Network Profiles > GlobalProtect IPSec Crypto.....	282
Network > Network Profiles > IKE Gateways.....	283
Network > Network Profiles > IPSec Crypto	289
Network > Network Profiles > IKE Crypto	290
Network > Network Profiles > Interface Mgmt	291
Network > Network Profiles > Monitor	292
Network > Network Profiles > Zone Protection.....	293
Network > Network Profiles > LLDP Profile.....	300
Network > Network Profiles > BFD Profile.....	301
Network > Network Profiles > QoS	303
Device.....	305
Device > Setup.....	306
Device > Setup > Management.....	307
Device > Setup > Operations.....	323
Device > Setup > HSM	331
Device > Setup > Services	334
Device > Setup > Content-ID.....	339
Device > Setup > WildFire	343
Device > Setup > Session	345
Device > High Availability	353
HA Lite.....	353
Important Considerations for Configuring HA	353
Configure HA Settings.....	354
Device > Config Audit.....	364

Device > Password Profiles365
Username and Password Requirements366
Device > Administrators367
Device > Admin Roles369
Device > Access Domain371
Device > Authentication Profile372
Device > Authentication Sequence375
Device > VM Information Sources376
Settings to Enable VM Information Sources for VMware ESXi and vCenter Servers377
Settings to Enable VM Information Sources for AWS VPC378
Device > Virtual Systems380
Device > Shared Gateways382
Device > Certificate Management383
Device > Certificate Management > Certificates384
Device > Certificate Management > Certificate Profile389
Device > Certificate Management > OCSP Responder391
Device > Certificate Management > SSL/TLS Service Profile392
Device > Certificate Management > SCEP393
Device > Response Pages396
Device > Log Settings398
Select Log Forwarding Destinations398
Define Alarm Settings399
Clear Logs401
Device > Server Profiles402
Device > Server Profiles > SNMP Trap403
Device > Server Profiles > Syslog405
Device > Server Profiles > Email407
Device > Server Profiles > NetFlow408
Device > Server Profiles > RADIUS409
Device > Server Profiles > TACACS+410
Device > Server Profiles > LDAP411
Device > Server Profiles > Kerberos413
Device > Server Profiles > DNS414
Device > Local User Database > Users415
Device > Local User Database > User Groups416
Device > Scheduled Log Export417
Device > Software418
Device > Dynamic Updates420
Device > Licenses423
Behavior on License Expiry424
Device > Support425
Device > Master Key and Diagnostics426

Table of Contents

User Identification	429
Device > User Identification > User Mapping	430
Enable WMI Authentication.....	431
Enable Client Probing	432
Enable Server Monitoring.....	433
Configure Cache Timeouts for User Mapping Entries.....	434
Enable NTLM Authentication.....	435
Enable Redistribution of User Mappings Among Firewalls.....	436
Manage Syslog Message Filters.....	436
Manage the User Ignore List	438
Monitor Servers	438
Define Subnetworks to Include/Exclude for User Mapping.....	440
Device > User Identification > User-ID Agents	442
Manage Access to User-ID Agents	442
Configure Access to User-ID Agents	443
Device > User Identification > Terminal Services Agents.....	444
Device > User Identification > Group Mapping Settings	445
Device > User Identification > Captive Portal Settings.....	448
 GlobalProtect	 451
Network > GlobalProtect > Portals	452
GlobalProtect Portals General Tab	453
GlobalProtect Portals Authentication Configuration Tab	454
GlobalProtect Portals Agent Configuration Tab	455
GlobalProtect Portals Satellite Configuration Tab	468
Network > GlobalProtect > Gateways.....	470
GlobalProtect Gateways General Tab	471
GlobalProtect Gateways Authentication Tab	472
GlobalProtect Gateways Agent Tab	472
GlobalProtect Gateways Satellite Configuration Tab	477
Network > GlobalProtect > MDM	480
Network > GlobalProtect > Block List	481
Objects > GlobalProtect > HIP Objects.....	482
HIP Objects General Tab	483
HIP Objects Mobile Device Tab	484
HIP Objects Patch Management Tab	485
HIP Objects Firewall Tab	486
HIP Objects Antivirus Tab	487
HIP Objects Anti-Spyware Tab	487
HIP Objects Disk Backup Tab	488
HIP Objects Disk Encryption Tab	488
HIP Objects Data Loss Prevention Tab	489
HIP Objects Custom Checks Tab	489
Objects > GlobalProtect > HIP Profiles	490
Device > GlobalProtect Client.....	492
Managing the GlobalProtect Agent Software	492
Setting Up the GlobalProtect Agent	493
Using the GlobalProtect Agent	494

Panorama Web Interface	495
Use the Panorama Web Interface.....	496
Commit Your Changes in Panorama.....	499
Defining Policies on Panorama	502
Logs and Reports on Panorama	503
Log Storage Partitions for a Panorama Virtual Appliance.....	504
Panorama > High Availability.....	505
Panorama > Administrators	507
Panorama > Admin Roles	509
Panorama > Access Domains.....	511
Panorama > Managed Devices	512
Managed Firewall Administration	512
Managed Firewall Information	513
Firewall Software and Content Updates.....	515
Firewall Backups.....	516
Panorama > Templates	517
Templates.....	517
Template Stacks	519
Panorama > Device Groups	520
Panorama > Managed Collectors.....	521
View Log Collector Information.....	521
Configure a Log Collector	522
Install a Software Update on a Log Collector.....	527
Panorama > Collector Groups	528
Configure a Collector Group.....	529
View Collector Group Information	532
Panorama > VMware Service Manager	533
Configure Access to the NSX Manager.....	533
Synchronize Panorama with the NSX Manager.....	535
Create Service Definitions.....	536
Panorama > Log Settings	538
Panorama > Scheduled Config Export	541
Panorama > Software	542
Manage Panorama Software Updates.....	542
Display Panorama Software Update Information	543
Panorama > Device Deployment.....	544
Manage Software and Content Updates	545
Display Software and Content Update Information	547
Schedule Dynamic Content Updates.....	548
Manage Firewall Licenses	549



Web Interface Basics

- ▲ [Firewall Overview](#)
- ▲ [Features and Benefits](#)
- ▲ [Management Interfaces](#)
- ▲ [Last Login Time and Failed Login Attempts](#)
- ▲ [Message of the Day](#)
- ▲ [Task Manager](#)
- ▲ [Language](#)
- ▲ [Alarms](#)
- ▲ [Commit Changes](#)
- ▲ [Lock Configurations](#)
- ▲ [Save Candidate Configurations](#)

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.

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 use 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 [User Identification](#)).
- **Threat prevention**—Threat prevention services that protect the network from viruses, worms, spyware, and other malicious traffic can be varied by application and traffic source (see [Objects > Security Profiles](#)).
- **URL filtering**—Outbound connections can be filtered to prevent access to inappropriate web sites (see [Objects > Security Profiles > URL Filtering](#)).
- **Traffic visibility**—Extensive reports, logs, and notification mechanisms provide detailed visibility into network application traffic and security events. The Application Command Center (ACC) in the web interface identifies the applications with the most traffic and the highest security risk (see [Monitor](#)).
- **Networking versatility and speed**—The Palo Alto Networks firewall can augment or replace your existing firewall and can be installed transparently in any network or configured to support a switched or routed environment. Multigigabit speeds and a single-pass architecture provide these services to you with little or no impact on network latency.
- **GlobalProtect**—The GlobalProtect™ software provides security for client systems, such as laptops that are used in the field, by allowing easy and secure login from anywhere in the world.
- **Fail-safe operation**—High availability (HA) support provides automatic failover in the event of any hardware or software disruption (see [Device > Virtual Systems](#)).
- **Malware analysis and reporting**—The WildFire™ 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 firewalls 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. For detailed step-by-step instructions on how to configure and manage the firewall, refer to the [PAN-OS Administrator's Guide](#).
- **CLI**—Text-based configuration and monitoring over Telnet, Secure Shell (SSH), or the console port. For information on how to use the CLI, including on information on how to find a command and get help on command syntax, refer to the [CLI Quick Start](#).
- **Panorama**—Palo Alto Networks product that provides web-based management, reporting, and logging for multiple firewalls. The Panorama web interface is similar to the firewall web interface but with additional management functions (for details, see to the [Panorama Administrator's Guide](#)).
- **XML API**—Provides a Representational State Transfer (REST)-based interface to access firewall 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. For details, refer to the [PAN-OS and Panorama XML API Usage Guide](#).

Last Login Time and Failed Login Attempts

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

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

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

Message of the Day

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

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



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

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

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

Task Manager

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

Field/Button	Description
Type	The type of operation, such as log request, license refresh, or commit. You can click certain types to see more details about the operation, such as warning messages.
Status	Indicates whether the operation is pending (such as commits with Queued status), in progress (such as log requests with Active status), completed, or failed. For commits in progress, the Status indicates the percentage of completion.
Start Time	The date and time when the operation started. For commit operations, the Start Time indicates when a commit was added to the commit queue.
Messages	Displays details about the operation. If the entry indicates that there are too many messages, you can click the operation Type to see the messages. For commit operations, the Messages include the dequeued time to indicate when PAN-OS started performing the commit. To see the description an administrator entered for a commit, click Commit Description . For details, see Commit Changes .
Action	Click x to cancel a pending commit.
Show	Display All tasks (default) or only Running tasks (in progress), and optionally filter the list by task type (Jobs , Reports , or Log Requests).
Clear Commit Queue	Cancel all pending commits (available only to predefined administrative roles).

Language

By default, the locale (such as Spanish) of the computer from which you log in to the firewall determines the language that the web interface displays. To change the **Language** (bottom of the web interface), select a **Language** from the drop-down and click **OK**. The web interface then refreshes using the new language.

Alarms

An alarm is a firewall-generated message indicating that the number of events of a particular type (for example, encryption and decryption failures) has exceeded the threshold configured for that event type (see [Define Alarm Settings](#)). When generating an alarm, the firewall creates an Alarm log and opens the System Alarms dialog to display the alarm. After closing the dialog, you can reopen it anytime by clicking **Alarms** () at the bottom of the web interface. To prevent the firewall from automatically opening the dialog for a particular alarm, select Unacknowledged Alarms and click **Acknowledge** to move the alarms to the Acknowledged Alarms list.

Commit Changes

Click **Commit** at the top right of the web interface to [commit, validate, or preview](#) your changes to the firewall configuration. Committing applies the candidate configuration to the running configuration, which activates all configuration changes since the last commit. To save, revert, import, export, or load configurations, select [Device > Setup > Operations](#).

The firewall queues commit requests so that you can initiate a new commit while a previous commit is in progress. The firewall performs the commits in the order they are initiated but prioritizes commits that the firewall initiates automatically, such as FQDN refreshes. If the queue already has the maximum number of administrator-initiated commits (which varies by platform), you must wait for the firewall to finish processing a pending commit before initiating a new commit. Use the [Task Manager](#) to cancel commits or see details about commits that are pending, in progress, completed, or failed.

In the Commit dialog, click **Advanced** to display the following options.

Field/Button	Description
Include Device and Network configuration	Select this option to commit changes to settings in the Device and Network tabs (enabled by default).
Include Shared Object configuration	Select this option to commit changes to shared objects (enabled by default). This option is available only on firewalls with multiple virtual systems.
Include Policy and Object configuration	Select this option to commit changes to settings in the Policy and Objects tabs (enabled by default). This option is available only on firewalls for which the multiple virtual systems capability is disabled.
Include Virtual System configuration	Select this option to commit changes to policies and objects in All virtual systems (default) or Select one or more virtual systems in the list (enabled by default). This option is available only on firewalls with multiple virtual systems.
Description	<p>Enter a description (up to 512 characters) for the commit. A brief summary of what changed in the configuration is useful to other administrators who might want to know this without performing a configuration audit (comparison).</p>  The System log for a commit event will truncate the description value if it exceeds 512 characters.
Preview Changes	<p>Click Preview Changes to 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 each highlighted difference. If you select All, the results include the entire configuration files. Changes are color-coded based on configurable settings: added (green), modified (yellow), and deleted (red). The Device > Config Audit feature performs the same function (see Device > Config Audit).</p>  Because the preview results display in a new window, your browser must allow pop-up windows. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-up windows.

Field/Button	Description
Validate Changes	Select this option 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. To control who can validate configurations, you can enable or disable the Validate option in Admin Role profiles.
Commit	Select this option to start the commit or, if other commits are pending, to add it to the commit queue.

Lock Configurations

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

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



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

Field/Button	Description
Admin	The username of the administrator who set the lock.
Location	On a firewall with more than one virtual system (vsys), the scope of the lock can a specific vsys or the Shared location.
Type	<p>The lock type can be:</p> <ul style="list-style-type: none"> Config Lock—Blocks other administrators from changing the candidate configuration. Only a superuser or the administrator who set the lock can remove it. Commit Lock—Blocks other administrators from committing changes made to the candidate configuration. The commit queue does not accept new commits until all locks are released. This lock prevents collisions that can occur when multiple administrators make changes during concurrent login sessions and one administrator finishes and initiates a commit before the other administrators have finished. The firewall automatically removes the lock after completing the commit for which the administrator set the lock. A superuser or the administrator who set the lock can also manually remove it.
Comment	Enter up to 256 characters of text. This is useful for other administrators who want to know the reason for the lock.
Created At	The date and time when an administrator set the lock.
Logged In	Indicates whether the administrator who set the lock is currently logged in.
Take a Lock	To set a lock, Take a Lock , select the Type , select the Location (multiple virtual system firewalls only), enter optional Comments , click OK , and then Close .
Remove Lock	To release a lock, select it, Remove Lock , click OK , and then Close .

Save Candidate Configurations

Click **Save** at the top right of the web interface to create a snapshot file (.snapshot.xml) of the candidate configuration or to overwrite the existing snapshot with your latest changes. If the firewall reboots before you commit your changes, you can then revert the candidate configuration to the current snapshot to restore changes you made between the last commit and the last snapshot. To revert to the snapshot, select **Device > Setup > Operations** and click **Revert to last saved configuration**. If you don't revert to the snapshot after a reboot, the candidate configuration will be the same as the last committed configuration (the running configuration).



Saving your changes to the candidate configuration does not activate those changes. You must [Commit Changes](#) to activate them.

If you want to save configuration changes without overwriting the default snapshot file (.snapshot.xml), select **Device > Setup > Operations**, click **Save named configuration snapshot**, and specify a different **Name** for the snapshot file.



Dashboard

The **Dashboard** widgets show general firewall or Panorama 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 administrator can remove and add individual widgets, as needed.

Click Refresh () to update the Dashboard or an individual widget. To change the automatic refresh interval, select an interval (1 min, 2 mins, 5 mins, or Manual). To add a widget to the Dashboard, select a category and then the widget name from the **Widgets** drop-down. To delete a widget, click Delete () in the title bar of the widget.

Dashboard Widget	Description
Application Widgets	
Top Applications	Displays the applications with the most sessions. The block size indicates the relative number of sessions (mouse-over the block to view the number), and the color indicates the security risk—from green (lowest) to red (highest). Click an application to view its application profile.
Top High Risk Applications	Similar to Top Applications, except that it displays the highest-risk applications with the most sessions.
ACC Risk Factor	Displays the average risk factor (1-5) for the network traffic processed over the past week. Higher values indicate higher risk.
System Widgets	
General Information	Displays the firewall or Panorama name, model, PAN-OS® or Panorama software version, the application, threat, and URL filtering definition versions, the current date and time, and the length of time since the last restart.
Interfaces (firewall only)	Indicates whether each interface is up (green), down (red), or in an unknown state (gray).
System Resources	Displays the Management CPU usage, Data Plane usage, and the Session Count, which displays the number of sessions established through the firewall or Panorama.
High Availability	If high availability (HA) is enabled, indicates the HA status of the local and peer firewall/Panorama—green (active), yellow (passive), or black (other). For more information about HA, refer to Device > Virtual Systems or Panorama > High Availability .
Locks	Shows configuration locks that administrators have set.
Logged In Admins	Displays the source IP address, session type (web interface or CLI), and session start time for each administrator who is currently logged in.
Logs Widgets	
Threat Logs	Displays the threat ID, application, and date and time for the last 10 entries in the Threat log. The threat ID is a malware description or URL that violates the URL filtering profile. Only entries from last 60 minutes are displayed.

Dashboard Widget	Description
URL Filtering Logs	Displays the description and date and time for the last 60 minutes in the URL Filtering log.
Data Filtering Logs	Displays the description and date and time for the last 60 minutes in the Data Filtering log.
Config Logs	Displays the administrator user name, client (web interface or CLI), and date and time for the last 10 entries in the Configuration log. Only entries from the last 60 minutes are displayed.
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.



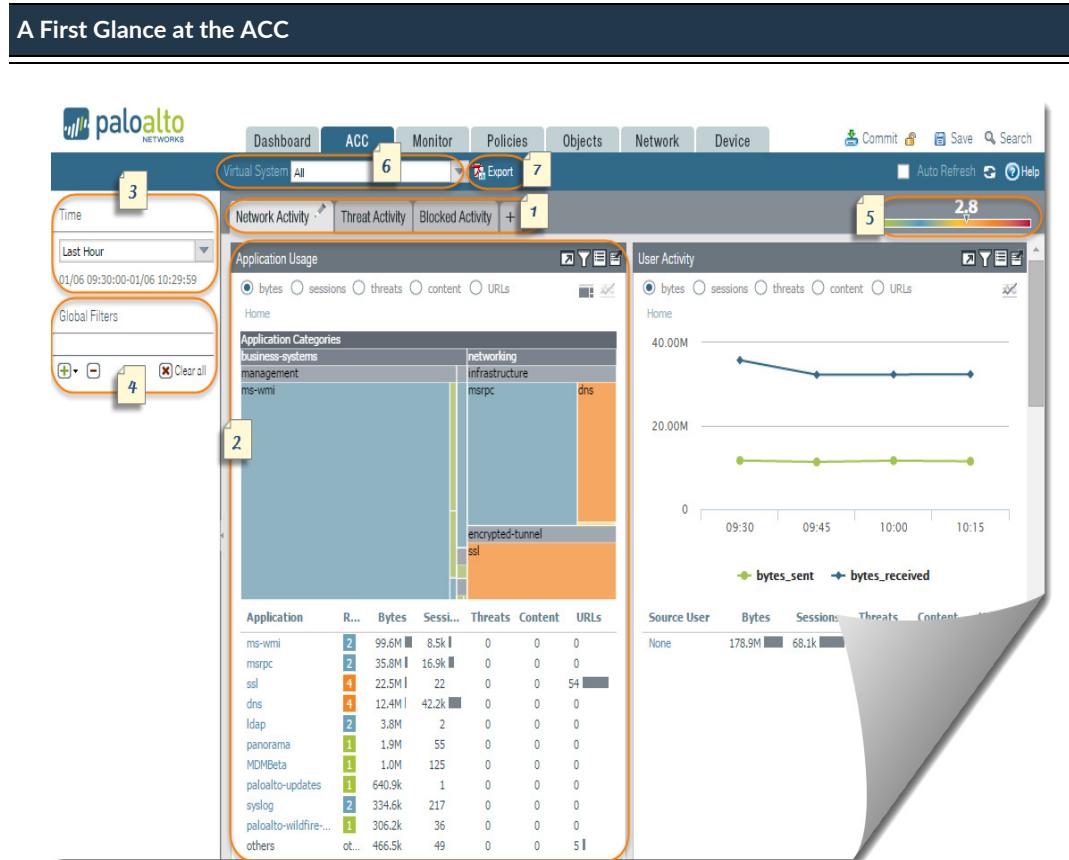
ACC

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
	ACC Views
	ACC Widgets
How do I interact with the ACC?	ACC Actions
	Working with Tabs and Widgets
	Working with Filters
Looking for more?	Use the Application Command Center 

A First Glance at the ACC

The following is a view of the ACC tab.



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 ACC 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 ACC Widgets .
3	Time	The charts and graphs in each widget provide a real-time and historic view. You can choose a custom range or use the predefined time periods that range from the last 15 minutes up to the last 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 ACC Actions .

A First Glance at the ACC

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.
6	Source	<p>The data source used for the display varies between the firewall and Panorama™.</p> <p>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.</p> <p>On Panorama, you can change the display to use Panorama or Remote Device Data (managed firewall data). When the data source is Panorama, you can filter the display for a specific device group.</p>
7	Export	You can export the widgets displayed in the current tab as a PDF.

ACC 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.

ACC 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.



Each widget is structured to display the following information.

ID	Widget	Description
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.

ID	Widget	Description
4	Actions	<p>The following are actions available in the title bar of a widget:</p> <p>Maximize view—Allows you to enlarge the widget and view it in a larger screen space. In the maximized view, you can see more than the top ten items displayed in the default screen width for the widget.</p> <p>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.</p> <p>Jump to logs—Allows you to directly navigate to the logs (Monitor > Logs > <Log type>). The logs are filtered using the time period for which the graph is rendered.</p> <p>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.</p> <p>Export—Allows you to export the graph as a PDF.</p>

For a description of each widget, see the details on [using the ACC](#).

ACC Actions

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

- [Working with Tabs and Widgets](#)
- [Working with Filters—Local Filters and Global Filters](#)

Working with Tabs and Widgets

The following table describes how to use and customize tabs and widgets.

Working with Tabs and Widgets	
• Add a custom tab.	<ol style="list-style-type: none"> 1. Select Add () along the list of tabs. 2. Add a View Name. This name will be used as the name for the tab. 3. You can add up to 5 tabs.
• Edit a tab.	<p>Select the tab and click edit next to the tab name to edit the tab.</p> <p>Example:  .</p>
• See what the widgets are included in a view.	<ol style="list-style-type: none"> 1. Select the view and click edit (). 2. Select the Add Widget drop-down to review selected widgets.

Working with Tabs and Widgets

<ul style="list-style-type: none"> Add a widget or a widget group. 	<ol style="list-style-type: none"> 1. Add a new tab or edit a predefined tab. 2. Select Add Widget, and then select the widget you want to add. You can select 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. <p> You cannot name a widget group.</p>
<ul style="list-style-type: none"> Delete a tab or a widget group/ widget. 	<ol style="list-style-type: none"> 1. To delete a custom tab, select the tab and click delete ().  You cannot delete a predefined tab. 2. To delete a widget or widget group, edit the tab and then click delete ([X]). You cannot undo a deletion.
<ul style="list-style-type: none"> Reset the default view. 	<p>On a predefined view, such as the Blocked Activity view, you can delete one or more widgets. If you want to reset the layout to include the default set of widgets for the tab, edit the tab and Reset View.</p>

Working with Filters—Local Filters and Global Filters

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

- **Local Filters**—Local filters are applied on a specific widget. A local filter allows you to interact with the graph and customize the display so that you can dig in to the details and access the information you want to monitor on a specific widget. You can apply a local filter in two ways—click into an attribute in the graph or table or select Set Filter within a widget. Set Filter allows you to set a local filter that is persistent across reboots.
- **Global filters**—Global filters are applied across the ACC. A global filter allows you to pivot the display around the details you care 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.
- **Add a widget filter to a global filter**—Hover over the attribute and click the arrow icon to the right of the attribute. This option allows you to elevate a local filter used in a widget, and apply the attribute globally to update the display across all the tabs on the ACC.
- **Define a global filter**—Define a filter using the **Global Filters** pane on the ACC.

The following table describes how to use filters in widgets.

Working with Filters	
<ul style="list-style-type: none"> Set a local filter. <p> You can also click an attribute in the table below the graph to apply it as a local filter.</p>	<ol style="list-style-type: none"> Select a widget and click Filter (). Add () filters you want to apply. Click Apply. These filters are persistent across reboots. <p> The number of local filters applied on a widget are indicated next to the widget name.</p>
<ul style="list-style-type: none"> Set a global filter from a table. 	Hover over an attribute in a table and click the arrow that appears to the right of the attribute.
<ul style="list-style-type: none"> Set a global filter using the Global Filters pane. 	Add () filters you want to apply.
<ul style="list-style-type: none"> Promote a local filter to as global filter. 	<ol style="list-style-type: none"> On any table in a widget, select an attribute. This sets the attribute as a local filter. To promote the filter to a global filter, hover over the attribute and click the arrow to the right of the attribute.
<ul style="list-style-type: none"> Remove a filter. 	<p>Click Remove () to remove a filter.</p> <ul style="list-style-type: none"> Global filters—Located in the Global Filters pane. Local filters—Click Filter () to bring up the Set Local Filters dialog and then select the filter and remove it.
<ul style="list-style-type: none"> Clear all filters 	<ul style="list-style-type: none"> Global filters—Clear All Global Filters. Local filters—Select a widget and click Filter () . Then Clear All in the Set Local Filters widget.
<ul style="list-style-type: none"> Negate filters 	<p>Select an attribute and Negate () a filter.</p> <ul style="list-style-type: none"> Global filters—Located in the Global Filters pane. Local filters—Click Filter () to bring up the Set Local Filters dialog add a filter, and then negate it.
<ul style="list-style-type: none"> View what filters are in use. 	<ul style="list-style-type: none"> Global filters—The number of global filters applied are displayed on the left pane under Global Filters. Local filters—The number of local filters applied on a widget are displayed next to the widget name. To view the filters, click Set Local Filters.



Monitor

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

- ▲ [Monitor > Logs](#)
- ▲ [Monitor > Automated Correlation Engine](#)
- ▲ [Monitor > Packet Capture](#)
- ▲ [Monitor > App Scope](#)
- ▲ [Monitor > Session Browser](#)
- ▲ [Monitor > Botnet](#)
- ▲ [Monitor > PDF Reports](#)
- ▲ [Monitor > Manage Custom Reports](#)
- ▲ [Monitor > Reports](#)

Monitor > Logs

The following topics provide additional information about monitoring logs.

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

Log Types

The firewall displays all logs so that role-based administration permissions are respected. Only the information that you have permission to see is included, and this might vary depending on the types of logs you are viewing. For information on administrator permissions, refer to [Device > Admin Roles](#).

Log Type	Description
Traffic	<p>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.</p> <p>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.</p> <p>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”.</p> <p>Drill down in traffic logs for more details on individual entries and artifacts:</p> <ul style="list-style-type: none"> Click Details () to view additional details about the session, such as whether an ICMP entry aggregates multiple sessions between the same source and destination (the Count value will be greater than one). On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash contained in a log entry and click the drop-down () to open the AutoFocus Threat Data for Log Artifacts of that artifact.

Log Type	Description
Threat	<p>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.</p> <p>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.</p> <p>Drill down in threat logs for more details on individual entries and artifacts:</p> <ul style="list-style-type: none"> Click Details () to view additional details about the threat, such as whether the entry aggregates multiple threats of the same type between the same source and destination (the Count value will be greater than one). On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash contained in a log entry and click the drop-down () to open the AutoFocus Threat Data for Log Artifacts of that artifact. If local packet captures are enabled, click Download () to access captured packets. To enable local packet captures, refer to the subsections under Objects > Security Profiles. To view more details about a threat or to quickly configure threat exemptions directly from the threat logs, click the threat name in the Name column. The Exempt Profiles list shows all custom Antivirus, Anti-spyware, and Vulnerability protection profiles. To configure an exemption for a threat signature, select the check box to the left of the security profile name and save your change. To add exemptions for IP Addresses (up to 100 IP addresses per signature), highlight the security profile, add the IP address(s) in the Exempt IP Addresses section and click OK to save. To view or modify the exemption, go to the associated security profile and click the Exceptions tab. For example, if the threat type is vulnerability, select Objects > Security Profiles > Vulnerability Protection, click the associated profile then click the Exceptions tab.
URL Filtering	<p>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.</p> <p>You can enable logging of the HTTP header options for the URL. Refer to Objects > Security Profiles > URL Filtering for information on defining URL filtering profiles.</p> <p>On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash contained in a log entry and click the drop-down () to open the AutoFocus Threat Data for Log Artifacts of that artifact.</p>
WildFire Submissions	<p>Displays logs for files that are uploaded and analyzed by the WildFire server. The server returns log data to the firewall after analysis, along with the analysis results.</p> <p>On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash (in the File Digest column) contained in a log entry and click the drop-down () to open the AutoFocus Threat Data for Log Artifacts for the artifact.</p>

Log Type	Description
Data Filtering	<p>Displays logs for the security policies with attached Data Filtering profiles, to help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall, and File Blocking profiles, that prevent certain file types from being uploaded or downloaded.</p> <p>To configure password protection for access the details for a log entry, click  . Enter the password and click OK. Refer to Device > Response Pages for instructions on changing or deleting the data protection password.</p> <p> The system prompts you to enter the password only once per session.</p>
Configuration	<p>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 interface or CLI), the type of command executed, whether the command succeeded or failed, the configuration path, and the values before and after the change.</p>
System	<p>Displays an entry for each system event. Each entry includes the date and time, the event severity, and an event description.</p>
HIP Match	<p>Displays information about security policies that apply to GlobalProtect™ clients. For more information, refer to Network > GlobalProtect > Portals.</p>
Alarms	<p>The alarms log records detailed information on alarms that are generated by the system. The information in this log is also reported in Alarms. Refer to Define Alarm Settings.</p>
Unified	<p>Displays the latest Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering log entries in a single view. The collective log view enables you to investigate and filter these different types of logs together (instead of searching each log set separately). Or, you can choose which log types to display: click the arrow to the left of the filter field and select traffic, threat, url, data, and/or wildfire to display only the selected log types.</p> <p>On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash contained in a log entry and click the drop-down () to open the AutoFocus Threat Data for Log Artifacts for that artifact.</p> <p>The firewall displays all logs so that role-based administration permissions are respected. When viewing Unified logs, only the logs that you have permission to see are displayed. For example, an administrator who does not have permission to view WildFire Submissions logs will not see WildFire Submissions log entries when viewing Unified logs. For information on administrator permissions, refer to Device > Admin Roles.</p> <p> You can use the Unified log set with the AutoFocus threat intelligence portal. Set up an AutoFocus search to add AutoFocus search filters directly to the Unified log filter field.</p>

Log Actions

The following table describes log actions.

Action	Description
Filter Logs	<p>Each log page has a filter field at the top of the page. You can add artifacts to the field, such as an IP address or a time range, to find matching log entries. The icons to the right of the field enable you to apply, clear, create, save, and load filters.</p>  <ul style="list-style-type: none"> Create a filter: <ul style="list-style-type: none"> Click an artifact in a log entry to add that artifact to the filter. Click Add () to define new search criteria. For each criterion, select the Connector that defines the search type (and or or), the Attribute on which to base the search, an Operator to define the scope of the search, and a Value for evaluation against log entries. Add each criterion to the filter field and Close when you finish. You can then apply () the filter. If the Value string matches an Operator (such as has or in), enclose the string in quotation marks to avoid a syntax error. For example, if you filter by destination country and use IN as a Value to specify INDIA, enter the filter as (dstloc eq "IN"). The log filter (<code>receive_time in last-60-seconds</code>) causes the number of log entries (and log pages) displayed to grow or shrink over time. Apply filters—Click Apply Filter () to display log entries that match the current filter. Delete filters—Click Clear Filter () to clear the filter field. Save a filter—Click Save Filter (), enter a name for the filter, and click OK. Use a saved filter—Click Load Filter () to add a saved filter to the filter field.
Export Logs	<p>Click Export to CSV () to export all logs matched to the current filter to a CSV-formatted report and continue to Download file. By default, the report contains up to 2,000 lines of logs. To change the line limit for generated CSV reports, select Device > Setup > Management > Logging and Reporting Settings > Log Export and Reporting and enter a new Max Rows in CSV Export value.</p>
Change Log Display	<ul style="list-style-type: none"> Change the automatic refresh interval—Select an interval from the interval drop-down (60 seconds, 30 seconds, 10 seconds, or Manual). Change the number and order of entries displayed per page—Log entries are retrieved in blocks of 10 pages. <ul style="list-style-type: none"> Use the paging controls at the bottom of the page to navigate through the log list. To change the number of log entries per page, select the number of rows from the per page drop-down (20, 30, 40, 50, 75, or 100). To sort the results in ascending or descending order, use the ASC or DESC drop-down. Resolve IP addresses to domain names—Select Resolve Hostname to begin resolving external IP addresses to domain names. Change the order in which logs are displayed—Select DESC to display logs in descending order beginning with log entries with the most recent Receive Time. Select ASC to display logs in ascending order beginning with log entries with the oldest Receive Time.

Action	Description
View Details for Individual Log Entries	<ul style="list-style-type: none"> To display additional details, click Details () for an entry. If the source or destination has an IP address to domain or username mapping defined in the Addresses page, the name is presented instead of the IP address. To view the associated IP address, move your cursor over the name. On a firewall with an active AutoFocus license, hover next to an IP address, filename, URL, user agent, threat name, or hash contained in a log entry and click the drop-down () to open the AutoFocus Threat Data for Log Artifacts for the artifact.

AutoFocus Threat Data for Log Artifacts

Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, and Unified logs include AutoFocus threat intelligence data to provide context for certain artifacts found in log entries, such as an IP address or a filename. In order to access the AutoFocus threat summary in firewall logs, first make sure that you have set up the firewall connection to AutoFocus (**Device > Setup > Management > AutoFocus**).



With Panorama, this feature allows you to view AutoFocus threat intelligence even for log entries from firewalls that are not connected to AutoFocus and/or are running PAN-OS 7.0 and earlier release versions.

When viewing the supported log types, click the drop-down () for the following artifacts in a log entry to find the latest AutoFocus findings and statistics for that artifact:

- An IP address.
- A URL.
- A user agent. (In Data Filtering logs, the user agent can be found in the User Agent column).
- A filename.
- A threat name.
- A SHA-256 hash. (In WildFire Submissions logs, the SHA-256 hashes for files the firewall submits to WildFire display in the File Digest column).

You can then review the AutoFocus Threat Intelligence Summary to quickly assess the pervasiveness and risk of an artifact. Click the link in the AutoFocus summary to open an AutoFocus search from the firewall. The AutoFocus portal opens in a new browser tab with the firewall artifact added as a search condition.

The AutoFocus summary for log artifacts previews the following details.

Field	Description
Passive DNS	Displays IP addresses, domains, URLs, and any recent passive DNS history for the artifact.
Matching Tags	Displays AutoFocus tags matched to the artifact. AutoFocus tags include your organization tags, public tags (tags shared by other AutoFocus users), and Unit 42 tags (tags that Palo Alto Networks creates to identify threats that pose a direct security risk).

Field	Description
Sessions	Displays the number of private sessions where detected samples contained the artifact. Private sessions are sessions running only on firewalls associated with your support account.
WildFire Verdicts	Displays the number of public and private grayware, benign, and malware samples with the artifact.
Recent WildFire Verdicts	Displays the latest private samples with which WildFire detected the artifact (including the sample file type, the date the sample was detected, and the WildFire verdict for the sample). Private samples are samples detected only on firewalls associated with your support account.

Monitor > Automated Correlation Engine

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

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

The 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

The following table provides additional information about the automated correlation engine.

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

Monitor > Automated Correlation Engine > Correlation Objects

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

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

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

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

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

Correlation Object 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.

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 the detailed log view, click Details () 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 Monitor > Automated Correlation Engine > Correlation Objects .
	Match Details —A summary of the match details that includes the match time, last update time on the match evidence, severity of the event, and an event summary.
Match Evidence	This tab includes all the evidence that corroborates the correlated event. It lists detailed information on the evidence collected for each session.

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

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

Monitor > Packet Capture

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



The packet capture feature is CPU-intensive and can degrade firewall performance. Only use this feature when necessary and make sure to turn it off after you 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
Where do I download a packet capture?	Packet Capture Overview
Looking for more?	
• Turn on extended packet capture for security profiles.	Device > Setup > Content-ID .
• Use packet capture to write custom application signatures.	See Doc-2015 . Note that this example uses a third-party app, but you can use the firewall to capture the required packets.
• Prevent a firewall admin from viewing packet captures.	Define Web Interface Administrator Access .
• See an example.	See Take Packet Captures .

Packet Capture Overview

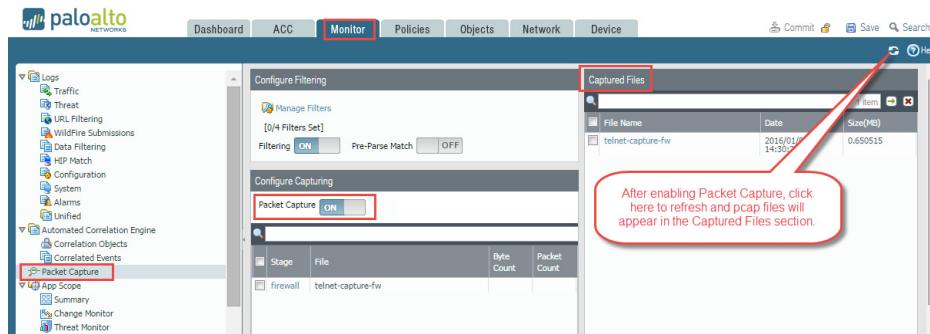
You can configure a Palo Alto Networks firewall to perform a custom packet capture or a threat packet capture.

- Custom Packet Capture—Capture packets for all traffic or traffic based on filters 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 () pcaps, select **Monitor > Threat**.

Building Blocks for a Custom Packet Capture

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



Custom Packet Capture Building Blocks	Configured In	Description
Manage Filters	Configure Filtering	<p>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.</p> <p>Click Add to add a new filter and configure the following fields:</p> <ul style="list-style-type: none"> • 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 this option to include IPv6 packets in the filter.

Custom Packet Capture Building Blocks	Configured In	Description
Filtering	Configure Filtering	After defining filters, set the Filtering to ON . If filtering is OFF , then all traffic is captured.
Pre-Parse Match	Configure Filtering	This option is for advanced troubleshooting purposes. After a packet enters the ingress port, it proceeds through several processing steps before it is parsed for matches against pre-configured filters. It is possible for a packet, due to a failure, to not reach the filtering stage. This can occur, for example, if a route lookup fails. Set the Pre-Parse Match setting to ON to emulate a positive match for every packet entering the system. This allows the firewall to capture packets that do not reach the filtering process. If a packet is able to reach the filtering stage, it is then processed according to the filter configuration and discarded if it fails to meet filtering criteria.
Packet Capture	Configure Capturing	Click the toggle switch to turn packet capture ON or OFF . You must select at least one capture stage. Click Add and specify the following: <ul style="list-style-type: none"> • Stage—Indicate the point at which to capture packets: <ul style="list-style-type: none"> - 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.
Captured Files	Captured Files	Contains a list of custom packet captures previously generated by the firewall. Click a file to download it to your computer. To delete a packet capture, select the packet capture and then Delete it. <ul style="list-style-type: none"> • File Name—Lists the packet capture files. The file names are based on the file name you specify for the capture stage • Date—Date the file was generated. • Size (MB)—The size of the capture file. After you turn on packet capture and then turn it off, you must click Refresh () before any new pcap files display in this list.

Custom Packet Capture Building Blocks	Configured In	Description
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

▲ Objects > Security Profiles

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

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

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



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

(Optional) To define the length of a threat packet capture based on the number of packets captured (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 Policy Overview](#).

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

Monitor > App Scope

- ▲ [App Scope Overview](#)
- ▲ [App Scope Summary Report](#)
- ▲ [App Scope Change Monitor Report](#)
- ▲ [App Scope Change Monitor Options](#)
- ▲ [App Scope Threat Monitor Report](#)
- ▲ [App Scope Threat Monitor Report Options](#)
- ▲ [App Scope Threat Map Report](#)
- ▲ [App Scope Threat Map Report Options](#)
- ▲ [App Scope Network Monitor Report](#)
- ▲ [App Scope Network Monitor Report Options](#)
- ▲ [App Scope Traffic Map Report](#)
- ▲ [App Scope Traffic Map Report Options](#)

App Scope Overview

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

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

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

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

Application Command Center Chart	Description
Summary	App Scope Summary Report
Change Monitor	App Scope Change Monitor Report
Threat Monitor	App Scope Threat Monitor Report
Threat Map	App Scope Threat Map Report

Application Command Center Chart	Description
Network Monitor	App Scope Network Monitor Report
Traffic Map	App Scope Traffic Map Report

App Scope Summary Report

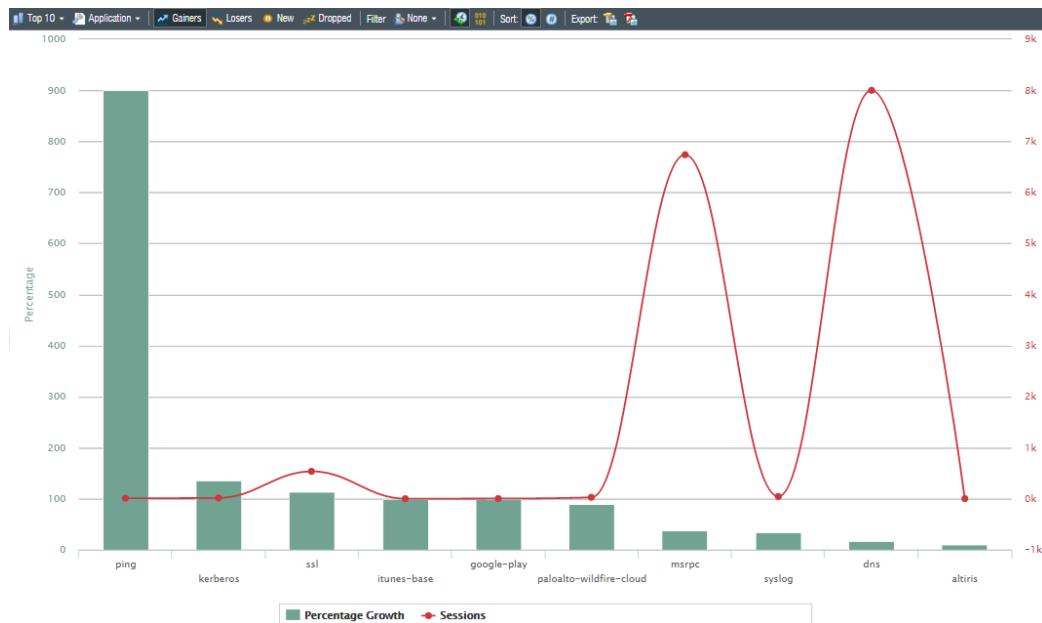
The Summary report displays charts for the top five gainers, losers, and bandwidth consuming applications, application categories, users, and sources.

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



App Scope Change Monitor Report

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



App Scope Change Monitor Options

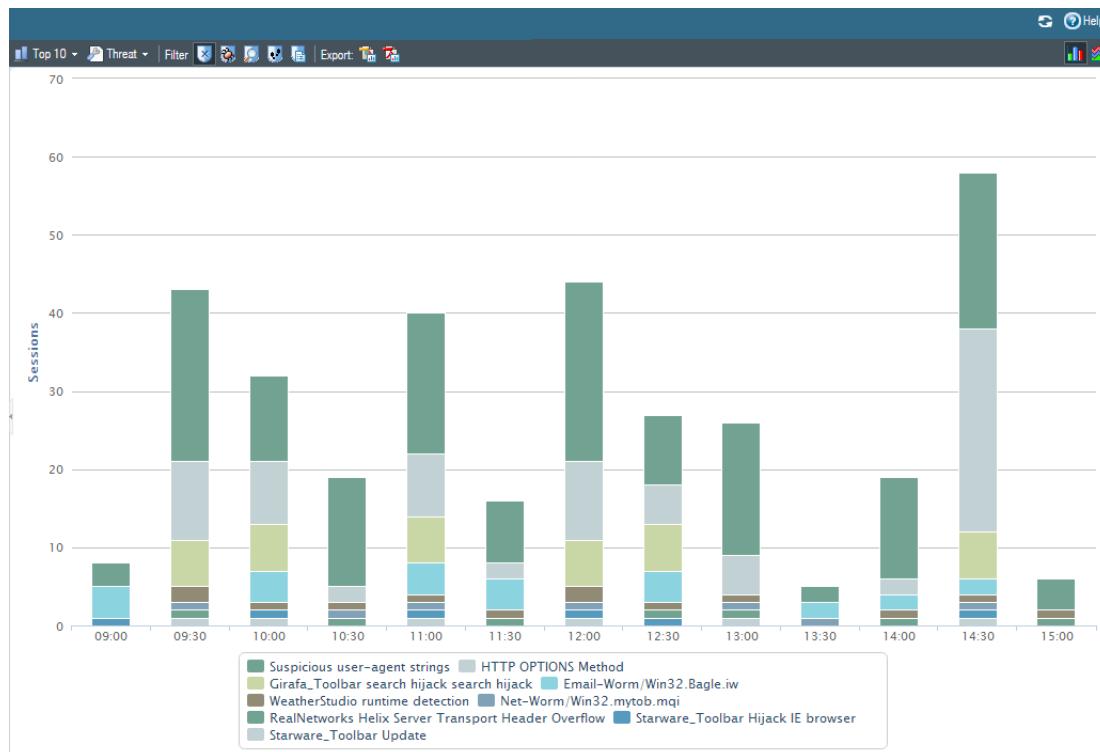
This report contains the following options.

Change Monitor Report Option	Description
Top Bar	
Top 10	Determines the number of records with the highest measurement included in the chart.
Application	Determines the type of item reported: Application, Application Category, Source, or Destination.
Gainers	Displays measurements of items that have increased over the measured period.
Losers	Displays measurements of items that have decreased over the measured period.
New	Displays measurements of items that were added over the measure period.
Dropped	Displays measurements of items that were discontinued over the measure period.
Filter None	Applies a filter to display only the selected item. None displays all entries.

Change Monitor Report Option	Description
Count Sessions and Count Bytes	Determines whether to display session or byte information.
Sort	Determines whether to sort entries by percentage or raw growth.
Export	Exports the graph as a .png image or as a PDF.
Bottom Bar	
Compare (interval)	Specifies the period over which the change measurements are taken.

App Scope Threat Monitor Report

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



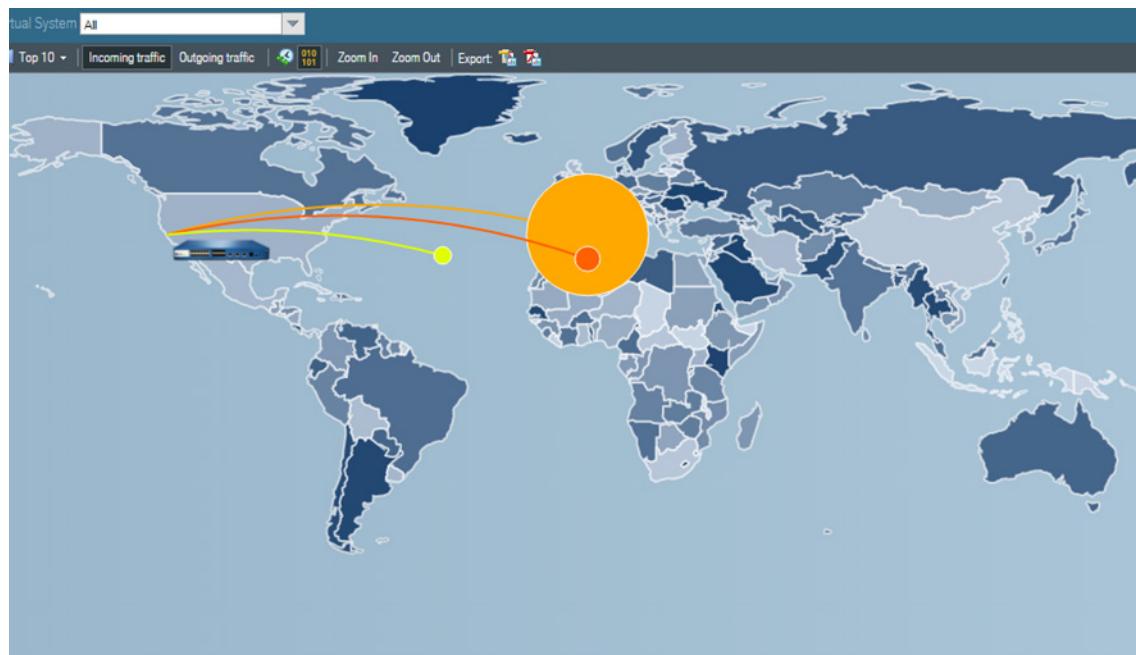
App Scope Threat Monitor Report Options

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

Threat Monitor Report Option	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.

App Scope Threat Map Report

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



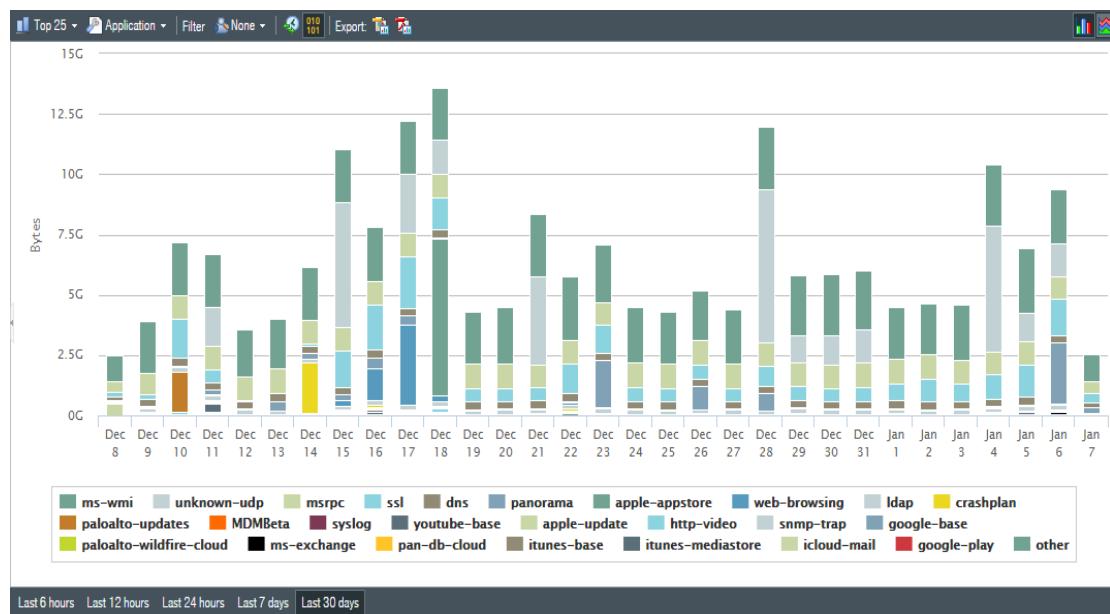
App Scope Threat Map Report Options

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

Threat Map Report Option	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.
Filter	Applies a filter to display only the selected type of items.
Zoom In and Zoom Out	Zoom in and zoom out of the map.
Export	Exports the graph as a .png image or as a PDF.
Bottom Bar	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indicates the period over which the measurements are taken.

App Scope Network Monitor Report

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



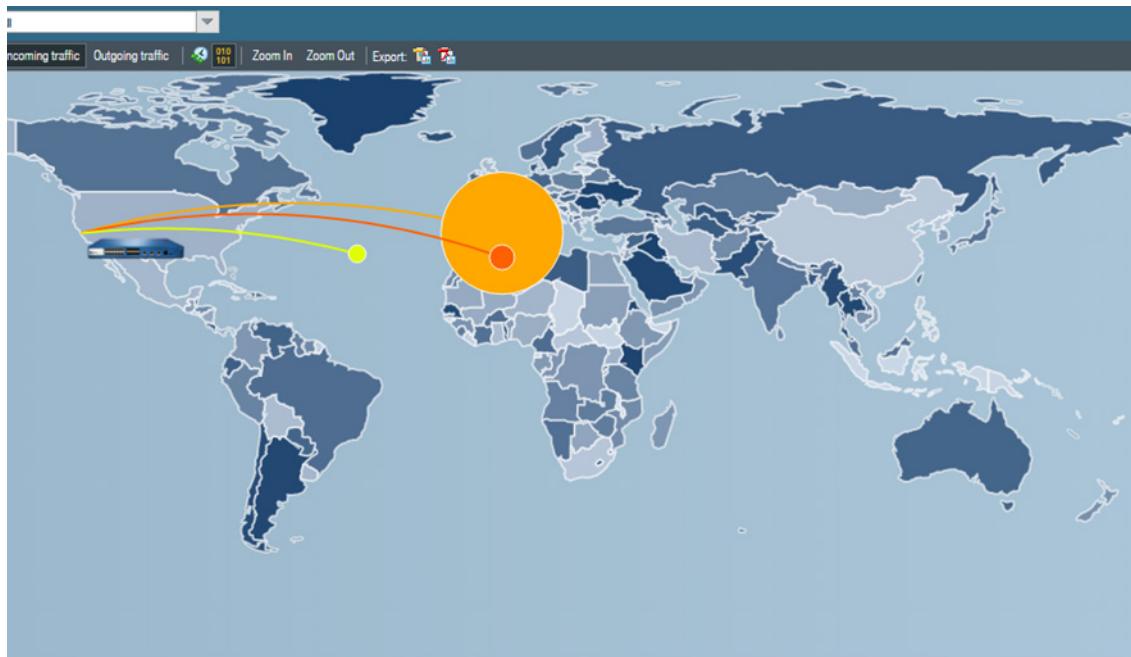
App Scope Network Monitor Report Options

The report contains the following options.

Network Monitor Report Option	Description
Top Bar	
Top 10 	Determines the number of records with the highest measurement included in the chart.
Application	Determines the type of item reported: Application, Application Category, Source, or Destination.
Filter 	Applies a filter to display only the selected item. None displays all entries.
	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.

App Scope Traffic Map Report

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



App Scope Traffic Map Report Options

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

Threat Map Report Option	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.
	Determines whether to display session or byte information.
Zoom In and Zoom Out	Zoom In and Zoom Out of the map.
Export	Export the graph as a .png image or as a PDF.
Bottom Bar	
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.

Monitor > Session Browser

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

Monitor > Botnet

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

- [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** and complete the following fields. To export a report, select it and **Export to PDF**, **Export to CSV**, or **Export to XML**.

Botnet Report Setting	Description
Test Run Time Frame	Select the time interval for the report— Last 24 Hours (default) or Last Calendar Day .
Run Now	Click Run Now to manually and immediately generate a report. The report displays in a new tab within the Botnet Report dialog.
No. of Rows	Specify the number of rows to display in the report (default is 100).
Scheduled	Select this option to automatically generate the report daily. By default, this option is enabled.
Query Builder	(Optional) Add queries to the Query Builder to filter the report output by attributes such as source/destination IP addresses, users, or zones. For example, if you know that traffic initiated from the IP address 192.0.2.0 contains no potential botnet activity, you can add <code>not (addr.src in 192.0.2.0)</code> as a query to exclude that host from the report output. <ul style="list-style-type: none">• Connector—Select a logical connector (and or or). If you select Negate, the report will exclude the hosts that the query specifies.• Attribute—Select a zone, address, or user that is associated with the hosts that the firewall evaluates for botnet activity.• Operator—Select an operator to relate the Attribute to a Value.• Value—Enter a value for the query to match.

Configuring the Botnet Report

▲ Monitor > Botnet > Configuration

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

Botnet Configuration Setting	Description
HTTP Traffic	<p>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.</p> <ul style="list-style-type: none"> • Malware URL visit (range is 2–1000; default is 5)—Identifies users communicating with known malware URLs based on malware and botnet URL filtering categories. • Use of dynamic DNS (range is 2–1000; default is 5)—Looks for dynamic DNS query traffic that might indicate malware, botnet communications, or exploit kits. Generally, using dynamic DNS domains is very risky. Malware often uses dynamic DNS to avoid IP blacklisting. Consider using URL filtering to block such traffic. • Browsing to IP domains (range is 2–1000; default is 10)—Identifies users who browse to IP domains instead of URLs. • Browsing to recently registered domains (range is 2–1000; default is 5)—Looks for traffic to domains that were registered within the past 30 days. Attackers, malware, and exploit kits often use newly registered domains. • Executable files from unknown sites (range is 2–1000; default is 5)—Identifies executable files downloaded from unknown URLs. Executable files are a part of many infections and, when combined with other types of suspicious traffic, can help you prioritize host investigations.
Unknown Applications	<p>Define the thresholds that determine whether the report will include traffic associated with suspicious Unknown TCP or Unknown UDP applications.</p> <ul style="list-style-type: none"> • Sessions Per Hour (range is 1–3600; default is 10)—The report includes traffic that involves up to the specified number of application sessions per hour. • Destinations Per Hour (range is 1–3600; default is 10)—The report includes traffic that involves up to the specified number of application destinations per hour. • Minimum Bytes (range is 1–200; default is 50)—The report includes traffic for which the application payload equals or exceeds the specified size. • Maximum Bytes (range is 1–200; default is 100)—The report includes traffic for which the application payload is equal to or less than the specified size.
IRC	Select this option to include traffic involving IRC servers.

Monitor > PDF Reports

- ▲ [Monitor > PDF Reports > Manage PDF Summary](#)
- ▲ [Monitor > PDF Reports > User Activity Report](#)
- ▲ [Monitor > PDF Reports > SaaS Application Usage](#)
- ▲ [Monitor > PDF Reports > Report Groups](#)
- ▲ [Monitor > PDF Reports > Email Scheduler](#)

Monitor > PDF Reports > Manage PDF Summary

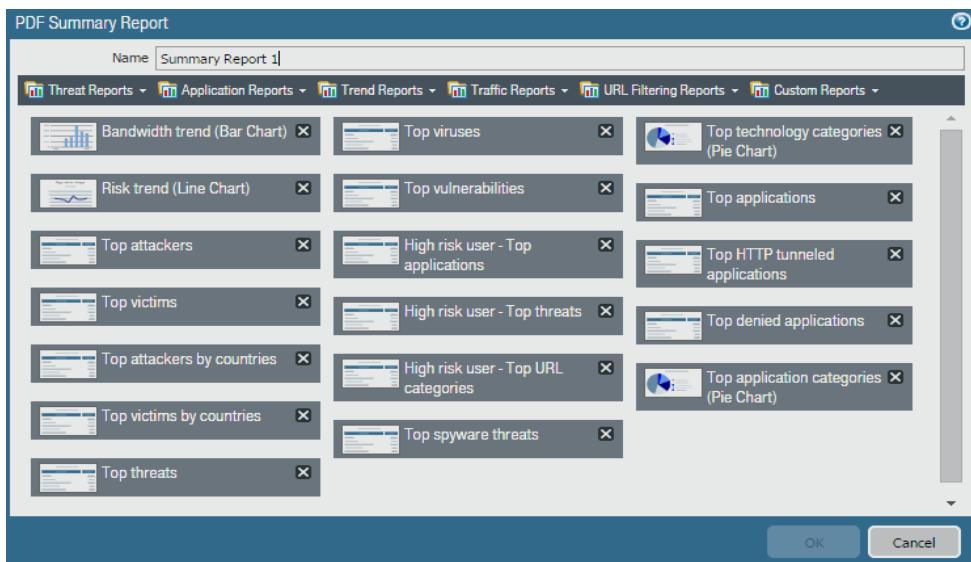
PDF summary reports contain information compiled from existing reports, based on data for the top 5 in each category (instead of top 50). They also contain trend charts that are not available in other reports.

PDF Summary Report



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

Managing PDF Reports



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

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



A maximum of 18 report elements is permitted. If you have 18 already, you must delete existing elements before you can add any.

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

To display PDF reports, select **Monitor > Reports** and click **PDF Summary Report** and click a report to open or save that report. You can also export a report using the options at the bottom of the page (**Export to PDF**, **Export to CSV**, or **Export to XML**) or click a day in the calendar to download a report for that day.



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

Monitor > PDF Reports > User Activity Report

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

User/Group Activity Report Setting	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	<p>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 (firewall) for each device group in order to retrieve user group information for generating the report.</p> <p>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).</p>
Time Period	Select the time frame for the report from the drop-down.
Include Detailed Browsing	<p>(Optional) Select this option to include detailed URL logs in the report.</p>  The detailed browsing information can include a large volume of logs (thousands) for the selected user or user group and cause a report to be very large.



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

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

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

Monitor > PDF Reports > SaaS Application Usage

Use this page to create a report that summarizes the SaaS application activity on your network. This predefined report presents a comparison on the sanctioned versus unsanctioned SaaS application usage on your network and you can use this information to help steer your users toward sanctioned applications. You can then enforce granular context and application-based policies for SaaS applications that you want to allow or block on your network.

To accurately generate this report, you must tag the sanctioned applications on your network (See [Actions Supported on Applications](#)). The firewall and Panorama consider any application without this predefined tag as unsanctioned for use on the network. It is important to know about the sanctioned applications and unsanctioned applications that are prevalent on your network because unsanctioned SaaS applications are a potential threat to information security; they are not approved for use on your network and can cause an exposure to threats and loss of private and sensitive data.

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

SaaS Application Usage Report Setting	Description
Name	Enter a name to identify the report (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Time Period	Select the time frame for the report from the drop-down: Last 7 days or Last 30 days .
Include detailed application category information in report	<p>The SaaS Application Usage PDF report is a two-part report. By default, both parts of the report are generated. The first part of the report (8 pages) focuses on the SaaS applications used on your network during the reporting period. Clear this option if you do not want the second part of the report that includes detailed information for SaaS and non-SaaS applications for each application subcategory listed in the first part of the report. This second part of the report includes the names of the top applications in each subcategory and information about users, files, bytes transferred, and threats generated from these applications.</p> <p>Without the detailed information, the report is eight-pages long.</p>

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

To schedule the report, see [Monitor > PDF Reports > Email Scheduler](#). On PA-200, PA-500, and PA-2000 Series firewalls, the SaaS Application Usage report is not sent as a PDF attachment in the email. Instead, the email includes a link you use to open the report in a web browser.



For generating an accurate and informative report, you need to tag the sanctioned applications consistently across firewalls with multiple virtual systems and device groups. If the same application is tagged as sanctioned in one virtual system and is not sanctioned in another or, on Panorama, if an application is unsanctioned in a parent device group but is tagged as sanctioned in a child device group (or vice versa), the SaaS Application Usage report will produce overlapping results.

Example: If Box is sanctioned on vsys1 and Google Drive is sanctioned on vsys2, Google Drive users in vsys1 will be counted as users of an unsanctioned SaaS application and Box users in vsys2 will be counted as users of an unsanctioned SaaS application. The key finding in the report will highlight that a total of two unique SaaS applications are discovered on the network with two sanctioned applications and two unsanctioned applications.

For more information on the report, see [Manage Reporting](#).

Monitor > PDF Reports > Report Groups

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

Report Group Setting	Description
Name	Enter a name to identify the report group (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Title Page	Select this option to include a title page in the report.
Title	Enter the name that will appear as the report title.
Report selection / Widgets	<p>For each report to include in the group, select the report in the left column and Add it to the right column. You can select the following report types:</p> <ul style="list-style-type: none">• Predefined Report• Custom Report• PDF Summary Report• CSV• Log View—Whenever you create a custom report, the firewall automatically creates a Log View report with the same name. The Log View report shows the logs that the firewall used to build the contents of the custom report. To include the log view data, when creating a report group, add your Custom Reports and then add the matching Log View reports. The aggregate report generated for the report group displays the custom report data followed by the log data. <p>After you save the report group, the Widgets column of the Report Groups page lists the reports you added to the group.</p>

To use the report group, refer to [Monitor > PDF Reports > Email Scheduler](#).

Monitor > PDF Reports > Email Scheduler

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

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

Email Scheduler Setting	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 Monitor > PDF Reports > Report Groups).
Email Profile	Select the profile that defines the email settings. Refer to Device > Server Profiles > Email for information on defining email profiles.
Recurrence	Select the frequency at which to generate and send the report.
Override Email Addresses	Enter an optional email address to use instead of the recipient specified in the email profile.

Monitor > Manage Custom Reports

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

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

Custom Report Setting	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 this option to run the report each night. The report then becomes available by selecting Monitor > Reports .
Columns	Select Available Columns to include in the custom report and add () them to Selected Columns. Select Up, Down, Top, and Bottom to reorder selected columns. As needed, you can also select and remove () previously selected columns.
Query Builder	To build a report query, specify the following and click Add . Repeat as needed to construct the full query. <ul style="list-style-type: none">• Connector—Choose the connector (and or or) to precede the expression you are adding.• Negate—Select this option to interpret the query as a negation. In the previous example, the negate option causes a match on entries that are not in the past 24 hours or are not from the untrust zone.• Attribute—Choose a data element. The available options depend on the choice of database.• Operator—Choose the criterion to determine whether the attribute applies (such as =). The available options depend on the choice of database.• Value—Specify the attribute value to match.

For more information, see [Generate Custom Reports](#) .

Monitor > Reports

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

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

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

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

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



Policies

This section describes the firewall web interfaces you can use to configure policies:

- ▲ [Policy Types](#)
- ▲ [Move or Clone a Policy Rule](#)
- ▲ [Policies > Security](#)
- ▲ [Policies > NAT](#)
- ▲ [Policies > QoS](#)
- ▲ [Policies > Policy Based Forwarding](#)
- ▲ [Policies > Decryption](#)
- ▲ [Policies > Application Override](#)
- ▲ [Policies > Captive Portal](#)
- ▲ [Policies > DoS Protection](#)

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 [Policies > Security](#).
- Network Address Translation (NAT) policies to translate addresses and ports, as needed. Refer to [Policies > NAT](#).
- Policy-based forwarding policies to override the routing table and specify an egress interface for traffic. Refer to [Policies > Policy Based Forwarding](#).
- Decryption policies to specify traffic decryption for security policies. Each policy can specify the categories of URLs for the traffic you want to decrypt. SSH decryption is used to identify and control SSH tunneling in addition to SSH shell access. Refer to [Policies > Decryption](#).
- Override policies to override the application definitions provided by the firewall. Refer to [Policies > Application Override](#).
- Quality of Service (QoS) policies to determine how traffic is classified for treatment when it passes through an interface with QoS enabled. Refer to [Policies > QoS](#).
- Captive portal policies to request authentication of unidentified users. Refer to [Policies > Captive Portal](#).
- Denial of service (DoS) policies to protect against DoS attacks and take protective action in response to rule matches. Refer to [Policies > DoS Protection](#).



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



Use the [Tag Browser](#) to view all the tags used in a rulebase. In rulebases with many rules, the tag browser simplifies the display by presenting the tags, color code, and the rule numbers in which tags are used.

Move or Clone a Policy Rule

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

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

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

Move/Clone Setting	Description
Selected Rules	Displays the Name and current Location (virtual system or device group) of the policy rules you selected for the operation.
Destination	Select the new location for the policy or object (a virtual system, device group, or Shared). The default value is the Virtual System or Device Group that you selected in the Policies or Objects tab.
Rule order	Select the rule position relative to other rules: <ul style="list-style-type: none">• Move top—The rule will precede all other rules.• Move bottom—The rule will follow all other rules.• Before rule—In the adjacent drop-down, select the subsequent rule.• After rule—In the adjacent drop-down, select the preceding rule.
Error out on first detected error in validation	Select this option (selected by default) to make the firewall or Panorama display the first error it finds and stop checking for more errors. For example, an error occurs if the Destination doesn't include an object that is referenced in the policy rule you are moving. If you clear this selection, the firewall or Panorama will find all errors before displaying them.

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 Policy Overview
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
	Overriding or Reverting a Security Policy Rule
Looking for more?	Security Policy 

Security Policy Overview

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

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**—Select the **General** tab to configure a name and description for the security policy.
- **Source**—Select the **Source** tab to define the source zone or source address from which the traffic originates.
- **User**—Select the **User** tab to enforce policy for individual users or a group of users. If you are using GlobalProtect with host information profile (HIP) enabled, you can also base the policy on information collected by GlobalProtect. For example, the user access level can be determined HIP that notifies the firewall about the user's local configuration. The HIP information can be used for granular access control based on the security programs that are running on the host, registry values, and many other checks such as whether the host has antivirus software installed.
- **Destination**—Select the **Destination** tab to define the destination zone or destination address for the traffic.
- **Application**—Select the **Application** tab to have the policy action occur based on an application or application group. An administrator can also use an existing App-ID signature and customize it to detect proprietary applications or to detect specific attributes of an existing application. Custom applications are defined in **Objects > Applications**.
- **Service/URL Category**—Select the **Service/URL Category** tab to specify a specific TCP and/or UDP port number or a URL category as match criteria in the policy.

- **Action**—Select the **Action** tab to determine the action that will be taken based on traffic that matches the defined policy attributes.

Building Blocks in a Security Policy

The following section describes each 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.

Building Block in a Security Rule	Configured In	Description
Rule number	N/A	Each rule is automatically numbered and the order changes as rules are moved. When you filter rules to match specific 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, firewall rules, and post-rules within a rulebase and reflects the rule sequence and its evaluation order.

Building Block in a Security Rule	Configured In	Description
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		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.
Type		Specifies whether the rule applies to traffic within a zone, between zones, or both: <ul style="list-style-type: none"> • universal (default)—Applies the rule to all matching interzone and intrazone traffic in the specified source and destination zones. For example, if you create a universal rule with source zones A and B and destination zones A and B, the rule would apply to all traffic within zone A, all traffic within zone B, and all traffic from zone A to zone B and all traffic from zone B to zone A. • intrazone—Applies the rule to all matching traffic within the specified source zones (you cannot specify a 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 Network > Zones . Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.
Source Address		Click Add to add source addresses, address groups, or regions (default is any). Select from the drop-down, or click Address , Address Group , or Regions at the bottom of the drop-down, and specify the settings.

Building Block in a Security Rule	Configured In	Description
Source User	User	<p>Click Add to choose the source users or groups of users subject to the policy. The following source user types are supported:</p> <ul style="list-style-type: none"> • 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. <p> If you are using a RADIUS server and not the User-ID agent, the list of users does not display; you must enter user information manually.</p>
Source HIP Profile		<p>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. The following source HIP profiles are supported:</p> <ul style="list-style-type: none"> • any—Include any endpoint regardless of HIP information. • select—Include selected HIP profiles as determined by the selection in this window. For example, you can add one HIP profile, a list of HIP profiles, or manually add a HIP profile. • no-hip—HIP information is not required. This setting enables access from third-party clients that cannot collect or submit HIP information.

Building Block in a Security Rule	Configured In	Description
Destination Zone	Destination	<p>Click Add to choose destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones.</p> <p>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.</p>  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		<p>Click Add to add destination addresses, address groups, or regions (default is any). Select from the drop-down, or click Address at the bottom of the drop-down, and specify address settings.</p>
Application	Application	<p>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.</p> <p>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 view application members directly from the policy without having to navigate to the Object tab.</p>

Building Block in a Security Rule	Configured In	Description
Service	Service/URL Category	<p>Select services to limit to specific TCP and/or UDP port numbers. Choose one of the following from the drop-down:</p> <ul style="list-style-type: none"> • 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 firewall 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. (Or select Objects > Services and Objects > Service Groups).
URL Category		<p>Select URL categories for the security rule.</p> <ul style="list-style-type: none"> • 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. Select Objects > External Dynamic Lists to define custom categories.

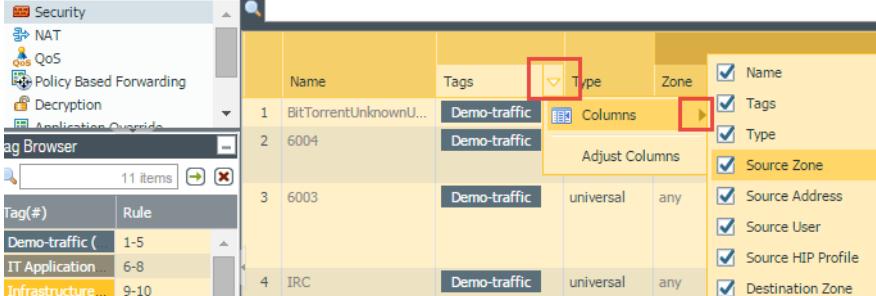
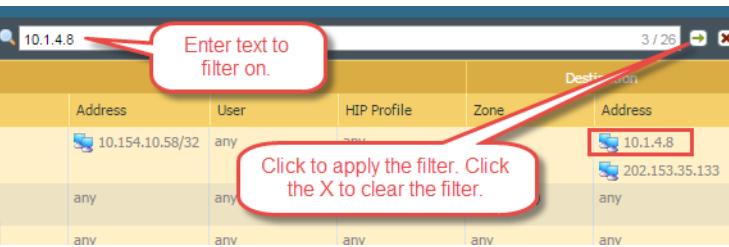
Building Block in a Security Rule	Configured In	Description
Action	Actions	<p>To specify the action for traffic that matches the attributes defined in a rule, select from the following actions:</p> <ul style="list-style-type: none"> • Allow—(default) Allows the traffic. • Deny—Blocks traffic, and enforces the default <i>Deny Action</i> 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. <p>To view the ICMP Unreachable Packet Rate configured on the firewall, view the Session Settings section in Device > Setup > Session.</p> <p>To override the default action defined on the predefined interzone and intrazone rules, see Overriding or Reverting a Security Policy Rule</p>
Profile Setting	Actions	<p>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.</p> <p>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.</p> <p>To define new profiles or profile groups, click New next to the appropriate profile or group (refer to Objects > Security Profile Groups).</p> <p>You can also attach security profiles (or profile groups) to the default rules.</p>

Building Block in a Security Rule	Configured In	Description
Options	Actions	<p>The Options tab includes the logging settings and the a combination of other options listed below.</p> <p>To generate entries in the local traffic log for traffic that matches this rule, select the following options:</p> <ul style="list-style-type: none"> • 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). <p> If the session start or end entries are logged, drop and deny entries are also logged.</p> <ul style="list-style-type: none"> • 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. <p>Note that the generation of threat log entries is determined by the security profiles. To define new log profiles, click New (refer to Objects > Log Forwarding).</p> <ul style="list-style-type: none"> • 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 Settings to Control Decrypted SSL Traffic). • QoS Marking—To change the Quality of Service (QoS) setting on packets matching the rule, select IP DSCP or 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 Quality of Service (QoS). • Disable Server Response Inspection—To disable packet inspection from the server to the client, select this option. 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

Select 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: <ul style="list-style-type: none"> 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 Move or Clone a Policy Rule.
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 Security Policy 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 Move or Clone a Policy Rule .
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 identify rules that have not been used since the last time the firewall was restarted, select Highlight Unused Rules . You can then decide whether to disable the rule or delete it. Rules not currently in use are displayed with a dotted yellow background. <div style="display: flex; align-items: center;">  Each firewall 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. </div>

Task	Description
Show/Hide columns	To show or hide the columns that display in the Policies pages, select this option next to the column name to toggle the display of each column. 
Apply filters	To apply a filter to the list, select from the Filter Rules drop-down. To add a value to define a filter, click the drop-down for the item and choose Filter .  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 Log Viewer .
	To display the current value by clicking the drop-down for the entry and choosing Value . 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 Address column, click the drop-down and select Value . This allows you to quickly view the members and the corresponding IP addresses for the address group without having to navigate to the Object tab.
	To find objects used within a policy based on their name or IP address, use the filter option. After you apply the filter, you will see only the items that match the filter. The filter also works with embedded objects. For example, when you filter on 10.1.4.8, only the policy that contains that address is displayed: 
Preview rules (Panorama only)	Use Preview Rules to view a list of the rules before you push the rules to the managed firewalls. Within each rulebase, the hierarchy of rules is visually demarcated for each device group (and managed firewall) to make it easier to scan through a large numbers of rules.

Overriding or Reverting a Security Policy Rule

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

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

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

Field to Use to Override a Default Security Rule	Description
General Tab	
Name	The Name that identifies the rule is read-only; you cannot override it.
Rule Type	The Rule Type is read-only; you cannot override it.
Description	The Description is read-only; you cannot override it.
Tag	Select Tags from the drop-down. A policy tag is a keyword or phrase that enables you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you might want to tag certain security policies with Inbound to DMZ, tag specific decryption policies with the words Decrypt or No-decrypt, or use the name of a specific data center for policies associated with that location.
Actions Tab	
Action Setting	Select the appropriate Action for traffic that matches the rule. <ul style="list-style-type: none"> • 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.

Field to Use to Override a Default Security Rule	Description
Profile Setting	<p>Profile Type—Assign profiles or profile groups to the security rule:</p> <ul style="list-style-type: none"> To specify the checking that the default security profiles perform, select Profiles and then select one or more of the individual Antivirus, Vulnerability Protection, Anti-Spyware, URL Filtering, File Blocking, Data Filtering, and 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 (Objects > Security Profiles) or profile groups (Objects > Security Profile Groups), click New in the drop-down for the corresponding profile or group.
Log Setting	<p>Specify any combination of the following options:</p> <ul style="list-style-type: none"> Log Forwarding—To forward the local traffic log and threat log entries to remote destinations, such as Panorama and syslog servers, select a Log Forwarding profile from the drop-down. Security profiles determine the generation of Threat log entries. To define a new Log Forwarding profile, select Profile in the drop-down (see Objects > Log Forwarding). To generate entries in the local traffic log for traffic that matches this rule, select the following options: <ul style="list-style-type: none"> 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).  <p>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.</p>

Policies > NAT

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

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

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

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

- [NAT General Tab](#)
- [NAT Original Packet Tab](#)
- [NAT Translated Packet Tab](#)
- [NAT Active/Active HA Binding Tab](#)

Looking for more?

See [NAT](#).

NAT General Tab

▲ Policies > NAT > General

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

NAT Rules - General Setting		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.

NAT Rules - General Setting	Description
NAT Type	<p>Specify the type of translation:</p> <ul style="list-style-type: none"> • ipv4—translation between IPv4 addresses. • nat64—translation between IPv6 and IPv4 addresses. • nptv6—translation between IPv6 prefixes. <p>You cannot combine IPv4 and IPv6 address ranges in a single NAT rule.</p>

NAT Original Packet Tab

▲ Policies > NAT > Original Packet

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

NAT Rules - Original Packet Setting	Description
Source Zone Destination Zone	<p>Select one or more source and destination zones for the original (non-NAT) packet (default is Any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones.</p> <p>You can specify multiple zones to simplify management. For example, you can configure settings so that multiple internal NAT addresses are directed to the same external IP address.</p>
Destination Interface	Specify the destination interface of packets the firewall translates. You can use the destination interface to translate IP addresses differently in the case where the network is connected to two ISPs with different IP address pools.
Service	Specify the service for which the firewall translates the source or destination address. To define a new service group, select Objects > Service Groups .
Source Address Destination Address	<p>Specify a combination of source and destination addresses for the firewall to translate.</p> <p>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.</p>

NAT Translated Packet Tab

▲ Policy > NAT > Translated Packet

Select 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.

You can also enable Destination Address Translation 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.

NAT Rules - Translated Packet Setting	Description
Source Address Translation	<p>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:</p> <ul style="list-style-type: none"> • 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 (Dynamic IP/Port Fallback)—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.

NAT Rules - Translated Packet Setting	Description
Bi-directional	<p>(Optional) Enable bidirectional translation if you want the firewall to create a corresponding translation (NAT or NPTv6) in the opposite direction of the translation you configure.</p>  <p>If you enable bidirectional translation, you must ensure that you have security policies in place to control the traffic in both directions. Without such policies, the bidirectional feature allows packets to be translated automatically in both directions.</p>
Destination Address Translation	<p>Enter an IP address or range of IP addresses and a translated port number (1-65535) to which the destination address and port number are translated. 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.</p> <p>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.</p>

NAT Active/Active HA Binding Tab

▲ Policies > NAT > Active/Active HA Binding

The Active/Active HA Binding tab is available only if the firewall is in a high availability (HA) active/active configuration. In this configuration, you must bind each source NAT rule (whether static or dynamic NAT) to Device ID 0 or Device ID 1. You typically configure device-specific NAT rules when the two HA peers have unique NAT IP address pools.

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

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

You must bind each destination NAT rule to either Device ID 0, Device ID 1, **both** (Device ID 0 and Device ID 1), or the **active-primary** firewall.

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

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

Looking for more?

See [NAT in Active/Active HA Mode](#).

Policies > QoS

Add [QoS policy](#) rules to define traffic to receive QoS treatment, and assign a [QoS class](#) for each QoS policy rule in order to apply that class of service to traffic matched to the rule as it exits a QoS-enabled interface.

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

To fully enable the firewall to provide QoS, also:

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

See [Quality of Service](#) for complete QoS workflows, concepts, and use cases.

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

QoS Policy Rule Setting	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).

QoS Policy Rule Setting	Description
Source Address	<p>Specify a combination of source IPv4 or IPv6 addresses for which the identified application can be overridden. To select specific addresses, choose Select from the drop-down and do any of the following:</p> <ul style="list-style-type: none"> Select this option next to the appropriate addresses  and/or address groups  in the Available column, and Add your selections to the Selected column. Enter the first few characters of a name in the search field to list all addresses and address groups that start with those characters. Selecting an item in the list enables this option in the Available column. Repeat this process as often as needed, and then click Add. Enter one or more IP addresses (one per line), with or without a network mask. The general format is: <code><ip_address>/<mask></code> To remove addresses, select them (Selected column) and click Delete or select any to clear all addresses and address groups. <p>To add new addresses that can be used in this or other policies, click New Address. To define new address groups, select Objects > Address Groups.</p>
Source User	Specify the source users and groups to which the QoS policy will apply.
Negate	Select this option to have the policy apply if the specified information on this tab does NOT match.
Destination Tab	
Destination Zone	Select one or more destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire).
Destination Address	<p>Specify a combination of source IPv4 or IPv6 addresses for which the identified application can be overridden. To select specific addresses, choose Select from the drop-down and do any of the following:</p> <ul style="list-style-type: none"> Select this option next to the appropriate addresses  and/or address groups  in the Available column, and Add your selections to the Selected column. Enter the first few characters of a name in the search field to list all addresses and address groups that start with those characters. Selecting an item in the list enables this option in the Available column. Repeat this process as often as needed, and then click Add. Enter one or more IP addresses (one per line), with or without a network mask. The general format is: <code><ip_address>/<mask></code> To remove addresses, select them (Selected column) and click Delete or select any to clear all addresses and address groups. <p>To add new addresses that can be used in this or other policies, click New Address.</p>
Negate	Select this option to have the policy apply if the specified information on this tab does NOT match.
Application Tab	

QoS Policy Rule Setting	Description
Application	<p>Select specific applications for the QoS rule. To define new applications or application groups, select Objects > Applications.</p> <p>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.</p> <p>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.</p>
Service/URL Category Tab	
Service	<p>Select services to limit to specific TCP and/or UDP port numbers. Choose one of the following from the drop-down:</p> <ul style="list-style-type: none"> • any—The selected applications are allowed or denied on any protocol or port. • application-default—The selected applications are allowed or denied only on their default ports defined by Palo Alto Networks®. This option is recommended for allow policies. • Select—Click Add. Choose an existing service or choose Service or Service Group to specify a new entry.
URL Category	<p>Select URL categories for the QoS rule.</p> <ul style="list-style-type: none"> • Select Any to ensure that a session can match this QoS rule regardless of the URL category. • To specify a category, click Add and select a specific category (including a custom category) from the drop-down. You can add multiple categories. Refer to Objects > External Dynamic Lists for information on defining custom categories.
DSCP/TOS Tab	
Any	<p>Select Any (default) to allow the policy to match to traffic regardless of the Differentiated Services Code Point (DSCP) value or the IP Precedence/Type of Service (ToS) defined for the traffic.</p>
Codepoints	<p>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.</p> <p>Continue to Add codepoints to match traffic to the QoS policy:</p> <ul style="list-style-type: none"> • 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	<p>Choose the QoS class to assign to the rule, and click OK. Class characteristics are defined in the QoS profile. Refer to Network > Network Profiles > QoS for information on configuring settings for QoS classes.</p>

QoS Policy Rule Setting	Description
Schedule	<ul style="list-style-type: none">• Select None for the policy rule to remain active at all times.• From the drop-down, select Schedule (calendar icon) to set a single time range or a recurring time range during which the rule is active.

Policies > Policy Based Forwarding

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

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

The following tables describe the policy-based forwarding settings:

- [Policy Based Forwarding General Tab](#)
- [Policy Based Forwarding Source Tab](#)
- [Policy Based Forwarding Destination/Application/Service Tab](#)
- [Policy Based Forwarding Forwarding Tab](#)

Looking for more?

See [Policy-Based Forwarding](#).

Policy Based Forwarding General Tab

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

Field	Description
Name	Enter a name to identify the rule. The name is case-sensitive and can have up to 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.

Policy Based Forwarding Source Tab

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

Field	Description
Source Zone	<p>To choose source zones (default is any), click Add and select from the drop-down. To define new zones, refer to Network > Zones.</p> <p>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.</p>  <p>Only Layer 3 type zones are supported for policy-based forwarding.</p>
Source Address	<p>Click Add to add source addresses, address groups, or regions (default is any). Select from the drop-down, or click Address, Address Group, or Regions at the bottom of the drop-down, and specify the settings.</p>
Source User	<p>Click Add to choose the source users or groups of users subject to the policy. The following source user types are supported:</p> <ul style="list-style-type: none"> • 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.  <p>If you are using a RADIUS server and not the User-ID Agent, the list of users does not display; you must enter user information manually.</p>

Policy Based Forwarding Destination/Application/Service Tab

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

Field	Description
Destination Address	Click Add to add destination addresses, address groups, or regions (default is any). By default, the rule applies to Any IP address. Select from the drop-down, or click Address , Address Group , or Regions at the bottom of the drop-down, and specify the settings.
Application/Service	<p>Select specific applications or services for the PBF rule. To define new applications, refer to Defining Applications. To define application groups, refer to Objects > Application Groups.</p>  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/71/pan-os/pan-os/policy/pbf.html . <p>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.</p>

Policy Based Forwarding Forwarding Tab

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

Field	Description
Action	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Forward—Specify the next hop IP address and egress interface (the interface that the packet takes to get to the specified next hop). • Forward To VSYS—Choose the virtual system to forward to from the drop-down. • Discard—Drop the packet. • No PBF—Do not alter the path that the packet will take. This option, excludes the packets that match the criteria for source/destination/application/service defined in the rule. Matching packets use the route table instead of PBF; the firewall uses the route table to exclude the matched traffic from the redirected port.
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.

Field	Description
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. To define new schedules, refer to Settings to Control Decrypted SSL Traffic .

Policies > Decryption

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

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

SSL forward proxy decryption requires the configuration of a trusted certificate that 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. Create a certificate on the **Device > Certificate Management > Certificates** page and then click the name of the certificate and select **Forward Trust Certificate**.



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:

- [Decryption General Tab](#)
- [Decryption Source Tab](#)
- [Decryption Destination Tab](#)
- [Decryption Service/URL Category Tab](#)
- [Decryption Options Tab](#)

Looking for more?

See [Decryption](#)

Decryption General Tab

Select 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.

Decryption Source Tab

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

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

Field	Description
Source User	<p>Click Add to choose the source users or groups of users subject to the policy. The following source user types are supported:</p> <ul style="list-style-type: none"> • 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.  If you are using a RADIUS server and not the User-ID Agent, the list of users does not display; you must enter user information manually.

Decryption Destination Tab

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

Field	Description
Destination Zone	<p>Click Add to choose destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, refer to Network > Zones.</p> <p>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.</p>
Destination Address	<p>Click Add to add destination addresses, address groups, or regions (default is any). Select from the drop-down, or click Address, Address Group, or Regions at the bottom of the drop-down, and specify the settings. Select Negate to choose any address except the configured ones.</p>

Decryption Service/URL Category Tab

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

Field	Description
Service	<p>Apply the decryption policy to traffic based on specific TCP port numbers. Choose one of the following from the drop-down:</p> <ul style="list-style-type: none"> • 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. (Or select Objects > Services and Objects > Service Groups).
URL Category Tab	<p>Select URL categories for the decryption rule.</p> <ul style="list-style-type: none"> • Choose any to match any sessions regardless of the URL category. • To specify a category, click Add and select a specific category (including a custom category) from the drop-down. You can add multiple categories. Refer to Defining Custom Categories for information on defining custom categories.

Decryption Options Tab

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

Field	Description
Action	Select decrypt or no-decrypt for the traffic.
Type	<p>Select the type of traffic to decrypt from the drop-down:</p> <ul style="list-style-type: none"> • SSL Forward Proxy—Specifies that the policy will decrypt client traffic destined for an external server. • SSH Proxy—Specifies that the policy will decrypt SSH traffic. This option allows you to control SSH tunneling in policies by specifying the ssh-tunnel App-ID. • SSL Inbound Inspection—Specifies that the policy will decrypt SSL inbound inspection traffic.
Decryption Profile	Attach a decryption profile to the policy rule in order to block and control certain aspects of the traffic. For details on creating a decryption profile, select Objects > Decryption Profile .

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.

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

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

To create a custom application with application override:

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

Use the following tables to configure an application override rule.

- [Application Override General Tab](#)
- [Application Override Source Tab](#)
- [Application Override Destination Tab](#)
- [Application Override Protocol/Application Tab](#)

Looking for more?

See [Use Application Objects in Policy](#).

Application Override General Tab

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

Field	Description
Name	Enter a name to identify the rule. The name is case-sensitive and can have up to 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.

Application Override Source Tab

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

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

Application Override Destination Tab

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

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

Application Override Protocol/Application Tab

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

Field	Description
Protocol	Select the protocol 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 Objects > Applications).

Policies > Captive Portal

Use the following tables 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 [Device > User Identification > Captive Portal Settings](#).

The following tables describe the captive portal policy settings:

- [Captive Portal General Tab](#)
- [Captive Portal Source Tab](#)
- [Captive Portal Destination Tab](#)
- [Captive Portal Service/URL Category Tab](#)
- [Captive Portal Action Tab](#)

Looking for more?

See [Map IP Addresses to Usernames Using Captive Portal](#).

Captive Portal General Tab

Select 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.

Captive Portal Source Tab

Select 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	<p>Specify the following information:</p> <ul style="list-style-type: none">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 Negate to choose any address except the configured ones. Click Add to specify multiple interfaces or zones.

Captive Portal Destination Tab

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

Field	Description
Destination	<p>Specify the following information:</p> <ul style="list-style-type: none">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 Negate to choose any address except the configured ones. Click Add to specify multiple interfaces or zones.

Captive Portal Service/URL Category Tab

Select 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: <ul style="list-style-type: none"> • 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. (Or select Objects > Services and Objects > Service Groups).
URL Category	Select URL categories for the captive portal rule. <ul style="list-style-type: none"> • 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. You can add multiple categories. Refer to Objects > External Dynamic Lists for information on defining custom categories.

Captive Portal Action Tab

Select the **Action** tab to select the method for authenticating Captive Portal users.

Field	Description
Action Setting	Select an action to take: <ul style="list-style-type: none"> • web-form—Present a Captive Portal page for the user to explicitly enter authentication credentials or use client certificate authentication. You specify the authentication method when configuring Captive Portal. • no-captive-portal—Allow traffic to pass without presenting a captive portal page for authentication. • browser-challenge—Transparently obtain user authentication credentials. If you select this action, you must enable Kerberos Single Sign-On (SSO) or NT LAN Manager (NTLM) authentication when you configure Captive Portal. If Kerberos SSO authentication fails, the firewall falls back to NTLM authentication. If you did not configure NTLM, or NTLM authentication fails, the firewall falls back to web-form authentication.

Policies > DoS Protection

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

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

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

Use this page to [Add](#), edit, or delete DoS Protection policy rules.

The following tables describe the captive portal policy settings:

- [DoS Protection General Tab](#)
- [DoS Protection Source Tab](#)
- [DoS Protection Destination Tab](#)
- [DoS Protection Option/Protection Tab](#)

Looking for more?

See [DoS Protection Against Flooding of New Sessions](#).

DoS Protection General Tab

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

Field	Description
Name	Enter a name to identify the 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 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.

DoS Protection Source Tab

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

Field	Description
Type	<p>Select the Type of source to which the DoS Protection policy rule applies:</p> <ul style="list-style-type: none"> • Interface—Apply the rule to traffic coming from the specified interface or group of interfaces. • Zone—Apply the rule to traffic coming from any interface in a specified zone. <p>Click Add to specify multiple interfaces or zones.</p>
Source Address	<p>Specify one or more source addresses to which the DoS Protection policy rule applies. Click Add to specify multiple addresses.</p> <p>Select Negate to choose any address except the configured ones.</p>
Source User	<p>Specify one or more source users to which the DoS Protection policy rule applies:</p> <ul style="list-style-type: none"> • 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—Include all authenticated users, which means any IP address with user data mapped. This option is equivalent to the “domain users” group on a domain. • unknown—Include all unauthenticated users, which means IP addresses that are not mapped to a user. For example, you could use unknown for guest level access to something because they will have an IP address on your network, but will not be authenticated to the domain and will not have IP to user mapping information on the firewall. • Select—Include 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. <p> If you are using a RADIUS server and not the User-ID Agent, the list of users does not display; you must enter user information manually.</p>

DoS Protection Destination Tab

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

Field	Description
Type	<p>Specify the type of destination to which the rule applies:</p> <ul style="list-style-type: none"> • Interface—Apply the DoS Protection policy rule to traffic coming from an interface or a group of interfaces. • Zone—Apply the DoS policy needs to be applied to traffic coming from all interfaces in a given zone. <p>Click Add to specify multiple interfaces or zones.</p>
Destination Address	<p>Specify one or more destination addresses to apply the DoS Protection policy rule to traffic to specific destination addresses. Click Add to specify multiple addresses.</p> <p>Select Negate to specify any address except the configured ones.</p>

DoS Protection Option/Protection Tab

Select the **Option/Protection** tab to configure options for the DoS Protection policy rule, such as the type of service (http or https) to which the rule applies, the action to take against packets that match the rule, and whether or not to trigger a log forward for matched traffic. You can define a schedule for when the rule is active.

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

Field	Description
Service	<p>Click Add and select one or more services to apply the DoS policy to only the configured services. The default is Any service.</p>
Action	<p>Select the action the firewall will take against packets that match the rule:</p> <ul style="list-style-type: none"> • Deny—Drop all packets that match the rule. • Allow—Permit all packets that match the rule. • Protect—Enforce protections (on packets that match the rule) specified in the DoS Protection profile applied to this rule. Packets that match the rule are counted toward the threshold rates in the DoS Protection profile, which in turn trigger an alarm, activate another action, and trigger packet drops when the maximum rate is exceeded.

Field	Description
Schedule	Specify the schedule when the DoS Protection policy rule is in effect. The default setting of None indicates no schedule; the policy is always in effect. Alternatively, select a schedule or create a new schedule to control when the DoS Protection policy rule is in effect. Enter a Name for the schedule. Select Shared to share this schedule with every virtual system on a multiple virtual system firewall. Select a Recurrence of Daily , Weekly , or Non-recurring . Add a Start Time and End Time in hours:minutes, based on a 24-hour clock.
Log Forwarding	If you want to trigger forwarding of threat log entries 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 an Aggregate DoS Protection profile, which specifies the threshold rates at which the incoming traffic triggers an alarm, activates an action, and exceeds a maximum rate. All incoming connections (the aggregate) count toward the thresholds specified in an Aggregate DoS Protection profile. See Objects > Security Profiles > DoS Protection . An Aggregate profile setting of None means there are no threshold settings in place for the aggregate traffic.
Classified	Select this option and specify the following: <ul style="list-style-type: none"> • Profile—Select a Classified DoS Protection profile or create a new DoS Protection profile to apply to this rule. • Address—Select whether incoming connections count toward the thresholds in the profile if they match the source-ip-only, destination-ip-only, or src-dest-ip-both. If you specify a Classified DoS Protection profile, only the incoming connections that match a source IP address, destination IP address, or source and destination IP address pair count toward the thresholds specified in the profile. For example, you can specify a Classified DoS Protection profile with a Max Rate of 100 and specify an Address setting of source-ip-only in the rule. The result would be a limit of 100 sessions at any given time for that particular source IP address. See Objects > Security Profiles > DoS Protection .



Objects

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

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

- ▲ [Move, Clone, Override, or Revert Objects](#)
- ▲ [Actions in Security Profiles and Custom Objects](#)
- ▲ [Objects > Addresses](#)
- ▲ [Objects > Address Groups](#)
- ▲ [Objects > Regions](#)
- ▲ [Objects > Applications](#)
- ▲ [Objects > Application Groups](#)
- ▲ [Objects > Application Filters](#)
- ▲ [Objects > Services](#)
- ▲ [Objects > Service Groups](#)
- ▲ [Objects > Tags](#)
- ▲ [Objects > GlobalProtect > HIP Objects](#)
- ▲ [Objects > GlobalProtect > HIP Profiles](#)
- ▲ [Objects > External Dynamic Lists](#)
- ▲ [Objects > Custom Objects](#)
- ▲ [Objects > Security Profiles](#)
- ▲ [Objects > Security Profile Groups](#)
- ▲ [Objects > Log Forwarding](#)
- ▲ [Objects > Decryption Profile](#)
- ▲ [Objects > Schedules](#)

Move, Clone, Override, or Revert Objects

See the following topics for options to modify existing objects:

- [Move or Clone an Object](#)
- [Override or Revert an Object](#)

Move or Clone an Object

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

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

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

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

Override or Revert an Object

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

- **Override an object**—Select the **Objects** tab, select the descendant **Device Group** that will have the overridden version, select the object, click **Override**, and edit the settings. You cannot override **Name** or **Shared** settings for an object.

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

Actions in Security Profiles and Custom Objects

You can specify how the firewall responds to threat events by defining an action in certain security profile ([Objects > Security Profiles](#)) or custom spyware and vulnerability signatures ([Objects > Custom Objects > Spyware/Vulnerability](#)). Palo Alto Networks defines a default action for threat signatures, though you can set a new action for the firewall to use to enforce a specific threat or types of threats:

- Set the action in Antivirus profile to define how the firewall treats worms, viruses, trojans and spyware downloads ([Objects > Security Profiles > Antivirus](#)).
- Set the action in an Anti-Spyware profile to define how the firewall treats attempts from spyware on compromised hosts to phone-home or beacon out to external command and control (C2) servers ([Objects > Security Profiles > Anti-Spyware Profile](#)).
- Set the action in a Vulnerability Protection profile to define how the firewall treats attempts to exploit system flaws or gain unauthorized access to systems ([Objects > Security Profiles > Vulnerability Protection](#)).
- Set the action for custom spyware and vulnerability signatures to define how the firewall treats threats that match these custom patterns ([Objects > Custom Objects > Spyware/Vulnerability](#)).

The following table describes actions you can perform on profiles and custom objects.

Action	Description	Antivirus Profile	Anti-Spyware profile	Vulnerability Protection Profile	Custom Objects—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 (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.  In cases where HTTP traffic or decrypted HTTPS traffic is blocked based on the Reset Client setting, a TCP reset is not sent to the client; instead, a block page is presented to inform the user that the file download is not permitted. However, if a file triggers the Reset Client action after it has already started to be transmitted to the client, the file transmission ceases and a TCP reset is sent.	✓	✓	✓	✓
Reset Server	For TCP, resets the server-side connection. For UDP, the connection is dropped.	✓	✓	✓	✓

Action	Description	Antivirus Profile	Anti-Spyware profile	Vulnerability Protection Profile	Custom Objects—Spyware and Vulnerability
Reset Both	<p>For TCP, resets the connection on both client and server ends. For UDP, the connection is dropped.</p>  In cases where HTTP traffic or decrypted HTTPS traffic is blocked based on the Reset Both setting, a TCP reset is not sent to the client; instead, a block page is presented to inform the user that the file download is not permitted. However, if a file triggers the Reset Both action after it has already started to be transmitted to the client, the file transmission ceases and a TCP reset is sent.	✓	✓	✓	✓
Block IP	This action blocks traffic from either a source or a source-destination pair; configurable for a specified period of time.	—	✓	✓	✓
Sinkhole	<p>This action directs DNS queries for malicious domains to a sinkhole IP address. To learn more, see Action on DNS queries.</p> <p>The action is available for Palo Alto Networks DNS signatures and for custom domains included in Objects > External Dynamic Lists.</p>	—	✓	—	—

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.

New Address Setting	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 option if you want the address object to be available to: <ul style="list-style-type: none">• Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the address object will be available only to the Virtual System selected in the Objects tab.• Every device group on Panorama. If you clear this selection, the address object will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the address in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.
Description	Enter a description for the object (up to 255 characters).

New Address Setting	Description
Type	<p>Specify an IPv4 or IPv6 address or address range, or FQDN.</p> <p>IP Netmask Enter the IPv4 or IPv6 address or IP address range. The format is <i>ip_address/mask</i> or <i>ip_address</i> where the <i>mask</i> is the number of significant binary digits used for the network portion of the address.</p> <p>IPv4 examples: “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.</p> <p>IPv6 examples: “2001:db8:123:1::1” or “2001:db8:123:1::/64”</p> <p>IP Range To specify an address range, select IP Range, and enter a range of addresses. The format is <i>ip_address-ip_address</i> where each address can be IPv4 or IPv6.</p> <p>Example: “2001:db8:123:1::1 - 2001:db8:123:1::22”</p> <p>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 Network > DNS Proxy object, if a proxy is configured.</p>
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 Objects > Tags .

Objects > Address Groups

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

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

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

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

Dynamic address groups can also include statically defined address objects. If you create an address object and apply the same tags that you have assigned to a dynamic address group, that dynamic address group will include all static and dynamic objects that match the tags. You can, therefore use tags to pull together both dynamic and static objects in the same address group.

- **Static Address Groups**—A static address group can include address objects that are static, dynamic address groups, or it can be a combination of both address objects and dynamic address groups.

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

Address Group	Description
Name	Enter a name that describes the address group (up to 63 characters). This name appears in the address list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this option if you want the address group to be available to: <ul style="list-style-type: none"> • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the address group will be available only to the Virtual System selected in the Objects tab. • Every device group on Panorama. If you clear this selection, the address group will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the address group in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.
Description	Enter a description for the object (up to 255 characters).

Address Group	Description
Type	<p>Select Static or Dynamic.</p> <p>To create a dynamic address group, use the match criteria to assemble the members to be included in the group. Define the Match criteria using the AND or OR operators.</p> <p> 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.</p> <p>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.</p>
Tags	Select or enter the tags that you wish to apply to this address group. For information on tags, see Objects > Tags .

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 table describes the region settings.

New Region Setting	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 this option and specify the values (xxx.xxxxxx format). This information is used in the traffic and threat maps for App-Scope. Refer to Monitor > Logs .
Addresses	Specify an IP address, range of IP addresses, or subnet to identify the region, using any of the following formats: <ul style="list-style-type: none">• x.x.X.X• x.x.x.x-y.y.y.y• x.x.x.x/n

Objects > Applications

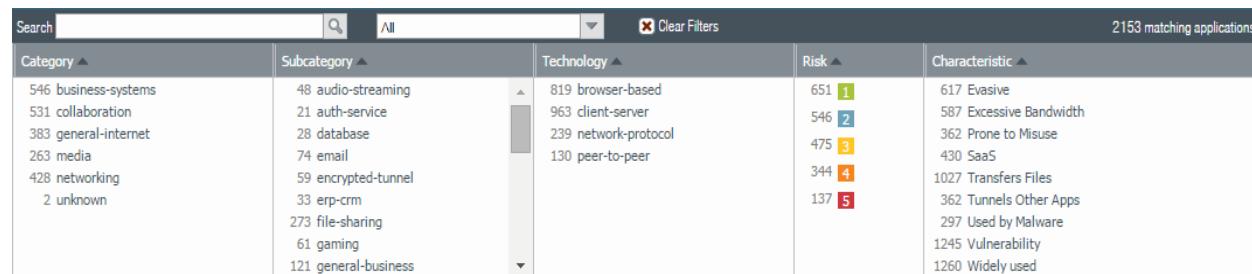
The following topics describe the **Applications** page.

What do you want to know?	See:
Understand the application settings and attributes displayed on the Applications page.	Applications Overview
	Actions Supported on Applications
Add a new application or modify an existing application.	Defining Applications

Applications Overview

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

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



The screenshot shows a table with the following columns: Category, Subcategory, Technology, Risk, and Characteristic. The table contains the following data:

Category	Subcategory	Technology	Risk	Characteristic
546 business-systems	48 audio-streaming	819 browser-based	651 1	617 Evasive
531 collaboration	21 auth-service	963 client-server	546 2	587 Excessive Bandwidth
383 general-internet	28 database	239 network-protocol	475 3	362 Prone to Misuse
263 media	74 email	130 peer-to-peer	344 4	430 SaaS
428 networking	59 encrypted-tunnel		137 5	1027 Transfers Files
2 unknown	33 erp-crm			362 Tunnels Other Apps
	273 file-sharing			297 Used by Malware
	61 gaming			1245 Vulnerability
	121 general-business			1260 Widely used



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

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

Application Detail	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.

Application Detail	Description
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 policy rule with a deny action. The default deny action can specify either a silent drop or a TCP reset. You can override this default action in Security policy.
Characteristics	
Evasive	Uses a port or protocol for something other than its originally intended purpose with the hope that it will traverse a firewall.
Excessive Bandwidth	Consumes at least 1 Mbps on a regular basis through normal use.
Prone to Misuse	Often used for nefarious purposes or is easily set up to expose more than the user intended.
SaaS	On the firewall, Software as a Service (SaaS) is characterized as a service where the software and infrastructure are owned and managed by the application service provider but where you retain full control of the data, including who can create, access, share, and transfer the data. Keep in mind that in the context of how an application is characterized, SaaS applications differ from web services. Web services are hosted applications where either the user doesn't own the data (for example, Pandora) or where the service is primarily comprised of sharing data fed by many subscribers for social purposes (for example, LinkedIn, Twitter, or Facebook).
Capable of File Transfer	Has the capability to transfer a file from one system to another over a network.
Tunnels Other Applications	Is able to transport other applications inside its protocol.
Used by Malware	Malware has been known to use the application for propagation, attack, or data theft, or is distributed with malware.
Has Known Vulnerabilities	Has publicly reported vulnerabilities.
Widely used	Likely has more than 1,000,000 users.

Application Detail	Description
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.
Classification	
Category	The application category will be one of the following: <ul style="list-style-type: none"> • business-systems • collaboration • general-internet • media • networking • unknown
Subcategory	The subcategory in which the application is classified. Different categories have different subcategories associated with them. For example, subcategories in the collaboration category include email, file-sharing, instant-messaging, Internet-conferencing, social-business, social-networking, voip-video, and web-posting. Whereas, subcategories in the business-systems category include auth-service, database, erp-crm, general-business, management, office-programs, software-update, and storage-backup.
Technology	The application technology will be one of the following: <ul style="list-style-type: none"> • client-server—An application that uses a client-server model where one or more clients communicate with a server in the network. • network-protocol—An application that is generally used for system-to-system communication that facilitates network operation. This includes most of the IP protocols. • peer-to-peer—An application that communicates directly with other clients to transfer information instead of relying on a central server to facilitate the communication. • browser-based—An application that relies on a web browser to function.
Risk	Assigned risk of the application. To customize this setting, click the Customize link, enter a value (1-5), and click OK .
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.

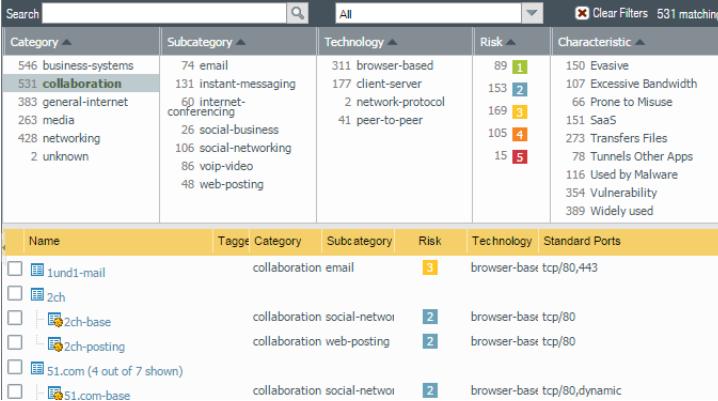
Application Detail	Description
UDP Timeout (seconds)	<p>Timeout, in seconds, for terminating a UDP application flow (range is 1-604800 seconds).</p> <p>To customize this setting, click the Customize link, enter a value, and click OK.</p>
TCP Half Closed (seconds)	<p>Maximum length of time, in seconds, 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).</p> <p>Default: If this timer is not configured at the application level, the global setting is used.</p> <p>If this value is configured at the application level, it overrides the global TCP Half Closed setting.</p>
TCP Time Wait (seconds)	<p>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).</p> <p>Default: If this timer is not configured at the application level, the global setting is used.</p> <p>If this value is configured at the application level, it overrides the global TCP Time Wait setting.</p>
App-ID Enabled	<p>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.</p>

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

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

Actions Supported on Applications

You can perform any of the following actions on the **Applications** page.

Action Supported for Applications	Description
Filter by application	<ul style="list-style-type: none"> To search for a specific application, enter the application name or description in the Search field and press Enter. The drop-down to the right of the search box allows you to search or filter for a specific application or view All applications, Custom applications, Disabled applications, or Tagged applications. <p>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.</p> <ul style="list-style-type: none"> To filter by application attributes displayed on the page; 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.  <p>The screenshot shows the Applications page with a search bar containing 'collaboration'. The results table has columns: Category, Subcategory, Technology, Risk, and Characteristic. The 'Category' column shows '546 business-systems' and '531 collaboration' (highlighted in yellow). The 'Technology' column shows '311 browser-based', '177 client-server', '2 network-protocol', and '41 peer-to-peer'. The 'Risk' column shows values 89, 153, 169, 105, and 15. The 'Characteristic' column lists various application types like Evasive, Excessive Bandwidth, Prone to Misuse, SaaS, Transfers Files, Tunnels Other Apps, Used by Malware, Vulnerability, and Widely used. Below the table, a list of specific applications is shown with columns: Name, Tagged Category, Subcategory, Risk, Technology, and Standard Ports. Applications listed include 1und1-mail (collaboration email), 2ch (collaboration social-networking), 2ch-base (collaboration web-posting), 51.com (collaboration social-networking), and 51.com-base (collaboration social-networking).</p> <ul style="list-style-type: none"> To filter on additional columns, select an entry in the other columns. The filtering is successive. First, the Category filters are applied, then the 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. To create a new application filter, see Objects > Application Filters.
Add a new application.	To add a new application, see Defining Applications .
View and/or customize application details.	Click the application name link, to view the application description including the standard port and characteristics of the application, risk among other details. For details on the application settings, see Defining Applications . If the icon to the left of the application name has a yellow pencil (), the application is a custom application.

Action Supported for Applications	Description
Disable an applications	You can Disable an application (or several applications) so that the application signature is not matched against traffic. Security rules defined to block, allow, or enforce a matching application are not applied to the application traffic when the app is disabled. You might choose to disable an application that is included with a new content release version because policy enforcement for the application might change when the application is uniquely identified. For example, an application that is identified as web-browsing traffic is allowed by the firewall prior to a new content version installation; after installing the content update, the uniquely identified application no longer matches the Security rule that allows web-browsing traffic. In this case, you could choose to disable the application so that traffic matched to the application signature continues to be classified as web-browsing traffic and is allowed.
Enable an application	Select a disabled application and Enable the application so that it can be enforced according to your configured security policies.
Import an application	To import an application, click Import . Browse to select the file, and select the target virtual system from the Destination drop-down.
Export an application	To export an application, select this option for the application and click Export . Follow the prompts to save the file.
Assess policy impact after installing a new content release.	Review Policies to assess the policy-based enforcement for applications before and after installing a content release version. Use the Policy Review dialog to review policy impact for new applications included in a downloaded content release version. The Policy Review dialog allows you to add or remove a pending application (an application that is downloaded with a content release version but is not installed on the firewall) to or from an existing Security policy; policy changes for pending applications do not take effect until the corresponding content release version is installed. You can also access the Policy Review dialog when downloading and installing content release versions on the Device > Dynamic Updates page.
Tag an application.	A predefined tag named sanctioned is available for you to tag SaaS applications. While a SaaS application is an application that is identified as Saas=yes in the details on application characteristics, you can use the sanctioned tag on any application. Select an application, click Tag Application , and, from the drop-down, select the predefined Sanctioned tag to identify any application that you want to explicitly allow on your network. When you then generate the SaaS Application Usage Report (see Monitor > PDF Reports > SaaS Application Usage), you can compare statistics on the application that you have sanctioned versus unsanctioned SaaS applications that are being used on your network. When you tag an application as sanctioned, the following restrictions apply: <ul style="list-style-type: none">• The sanctioned tag cannot be applied to an application group.• The sanctioned tag cannot be applied at the Shared level; you can tag an application only per device group or per virtual system.• The sanctioned tag cannot be used to tag applications included in a container app, such as facebook-mail, which is part of the facebook container app. You can also Remove tag or Override tag . The override option is only available on a firewall that has inherited settings from a device group pushed from Panorama.

Defining Applications

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

New Application Setting	Description
Configuration Tab	
Name	Enter the application name (up to 31 characters). This name appears in the applications list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, periods, hyphens, and underscores. The first character must be a letter.
Shared	Select this option if you want the application to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the application will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the application will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the application in descendant device groups by overriding its inherited values. This selection 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 ACC).
Subcategory	Select the application subcategory, such as email or database . The subcategory is used to generate the Top Ten Application Categories chart and is available for filtering (refer to ACC).
Technology	Select the technology for the application.
Parent App	Specify a parent application for this application. This setting applies when a session matches both the parent and the custom applications; however, the custom application is reported because it is more specific.
Risk	Select the risk level associated with this application (1=lowest to 5=highest).
Characteristics	Select the application characteristics that may place the application at risk. For a description of each characteristic, refer to Characteristics .
Advanced Tab	
Port	If the protocol used by the application is TCP and/or UDP, select Port and enter one or more combinations of the protocol and port number (one entry per line). The general format is <code><protocol>/<port></code> where the <code><port></code> 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.

New Application Setting	Description
IP Protocol	To specify an IP protocol other than TCP or UDP, select IP Protocol , and enter the protocol number (1 to 255).
ICMP Type	To specify an Internet Control Message Protocol version 4 (ICMP) type, select ICMP Type and enter the type number (range is 0-255).
ICMP6 Type	To specify an Internet Control Message Protocol version 6 (ICMPv6) type, select ICMP6 Type and enter the type number (range is 0-255).
None	To specify signatures independent of protocol, select None .
Timeout	Enter the number of seconds before an idle application flow is terminated (range is 0-604800 seconds). A zero indicates that the default timeout of the application will be used. This value is used for protocols other than TCP and UDP in all cases and for TCP and UDP timeouts when the TCP timeout and UDP timeout are not specified.
TCP Timeout	Enter the number of seconds before an idle TCP application flow is terminated (range is 0-604800 seconds). A zero indicates that the default timeout of the application will be used.
UDP Timeout	Enter the number of seconds before an idle UDP application flow is terminated (range is 0-604800 seconds). A zero indicates that the default timeout of the application will be used.
TCP Half Closed	Enter the maximum length of time that a session remains in the session table, between receiving the first FIN and receiving the second FIN or RST. If the timer expires, the session is closed. Default: If this timer is not configured at the application level, the global setting is used (range is 1-604800 seconds). If this value is configured at the application level, it overrides the global TCP Half Closed setting.
TCP Time Wait	Enter the maximum length of time that a session remains in the session table after receiving the second FIN or a RST. If the timer expires, the session is closed. Default: If this timer is not configured at the application level, the global setting is used (range is 1-600 seconds). If this value is configured at the application level, it overrides the global TCP Time Wait setting.
Scanning	Select the scanning types that you want to allow based on Security Profiles (file types, data patterns, and viruses).

New Application Setting	Description
Signature Tab	
Signatures	<p>Click Add to add a new signature, and specify the following information:</p> <ul style="list-style-type: none"> • 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. <p>Specify the conditions that identify the signature. These conditions are used to generate the signature that the firewall uses to match the application patterns and control traffic:</p> <ul style="list-style-type: none"> • To add a condition, select Add AND Condition or Add OR Condition. To add a condition within a group, select the group and then click Add Condition. • Select an Operator from the drop-down. The options are Pattern Match, Greater Than, Less Than, and Equal To and specify the following options: <ul style="list-style-type: none"> • For Pattern Match only: <ul style="list-style-type: none"> – Context—Select from the available contexts. These contexts are updated using dynamic content updates. – Pattern—Specify a regular expression to specify unique string context values that apply to the custom application. As a best practice, perform a packet capture to identify the context. See Pattern Rules Syntax for pattern rules for regular expressions. • For Greater Than, Less Than only: <ul style="list-style-type: none"> – Context—Select from the available contexts. These contexts are updated using dynamic content updates – Value—Specify a value to match on (range is 0-4294967295). – Qualifier and Value—(Optional) Add qualifier/value pairs. • For Equal To only: <ul style="list-style-type: none"> – Context—Select from unknown requests and responses for TCP or UDP (for example, unknown-req-tcp) or additional contexts that are available through dynamic content updates (for example, dnp3-req-func-code). For unknown requests and responses for TCP or UDP, specify – Position—Select between the first four or second four bytes in the payload. – Mask—Specify a 4-byte hex value, for example, 0xffffffff00. – Value—Specify a 4-byte hex value, for example, 0xaabbccdd. – For all other contexts, specify a Value that is pertinent to the application. <p>To move a condition within a group, select the condition and Move Up or Move Down. To move a group, select the group and Move Up or Move Down. You cannot move conditions from one group to another.</p>



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

Objects > Application Groups

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

New Application Group Setting	Description
Name	Enter a name that describes the application group (up to 31 characters). This name appears in the application list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this option if you want the application group to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the application group will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the application group will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the application group in descendant device groups by overriding its inherited values. This selection 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.

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 Collaboration category, click **collaboration**.

Search		All	Clear Filters 531 matching	
Category	Subcategory	Technology	Risk	Characteristic
546 business-systems	74 email	311 browser-based	89 1	150 Evasive
531 collaboration	131 instant-messaging	177 client-server	153 2	107 Excessive Bandwidth
383 general-internet	60 internet-conferencing	2 network-protocol	169 3	66 Prone to Misuse
263 media	26 social-business	41 peer-to-peer	105 4	151 SaaS
428 networking	106 social-networking		15 5	273 Transfers Files
2 unknown	86 voip-video			78 Tunnels Other Apps
	48 web-posting			116 Used by Malware
				354 Vulnerability
				389 Widely used
Name	Tags	Category	Subcategory	Risk
<input type="checkbox"/> 1und1-mail		collaboration	email	3
<input type="checkbox"/> 2ch				
<input type="checkbox"/> 2ch-base		collaboration	social-networking	2
<input type="checkbox"/> 2ch-posting			web-posting	2
<input type="checkbox"/> 51.com (4 out of 7 shown)				

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

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

Objects > Services

When you define security policies for specific applications, you can select one or more services to limit the port numbers the applications can use. The default service is **any**, which allows all TCP and UDP ports.

The HTTP and HTTPS services are predefined, but you can add additional service definitions. Services that are often assigned together can be combined into service groups to simplify the creation of security policies (refer to [Objects > Service Groups](#)).

The following table describes the service settings.

Service Setting	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 option if you want the service object to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the service object will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the service object will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the service object in descendant device groups by overriding its inherited values. This selection 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.

Objects > Service Groups

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

The following table describes the service group settings.

Service Group Setting	Description
Name	Enter the service group name (up to 63 characters). This name appears in the services list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this option if you want the service group to be available to: <ul style="list-style-type: none">Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the service group will be available only to the Virtual System selected in the Objects tab.Every device group on Panorama. If you clear this selection, the service group will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the service group in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.
Service	Click Add to add services to the group. Select from the drop-down or click Service at the bottom of the drop-down and specify the settings. Refer to Objects > Services for a description of the settings.

Objects > Tags

Tags allow you to group objects using keywords or phrases. Tags can be applied to address objects, address groups (static and dynamic), zones, services, service groups, and to policy rules. You can use 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.

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

What do you want to know?	See:
How do I create tags?	Create Tags
What is the tag browser?	Use the Tag Browser
Search for rules that are tagged.	
Group rules using tags.	
View tags used in policy.	Manage Tags
Apply tags to policy.	
Looking for more?	See Policy .

Create Tags

Select **Objects > Tags** 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.

Tag Setting	Description
Name	Enter a unique tag name (up to 127 characters). The name is not case-sensitive.
Shared	Select this option if you want the tag to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the tag will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the tag will be available only to the Device Group selected in the Objects tab.

Tag Setting	Description
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the tag in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.
Color	Select a color from the color palette in the drop-down. The default value is None.
Comments	Add a label or description to remind you what the tag is used for.

- **Add a tag**—To add a new tag, click **Add** and then fill in the following fields:
You can also create a new tag when you create or edit policy in the **Policies** tab. The tag is automatically created in the Device Group or Virtual System that is currently selected.
- **Edit a tag**—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. You cannot delete a predefined tag.
- **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 firewalls 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 this selection 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, this option is enabled and the validation process stops when the first error is detected and only displays the error.
- **Override or Revert a tag (Panorama only)**—The **Override** option is available 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 tag browser options.

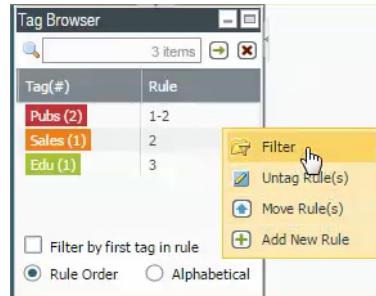
Tag Browser Option	Description
Tag (#)	Displays the label and the rule number or range of numbers in which the tag is used contiguously. Hover over the label to see the location where the rule was defined. The location can be inherited from the Shared location, a device group, or a virtual system.
Rule	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 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 you can perform using the tag browser.

Manage Tags	
<ul style="list-style-type: none"> • Tag a rule. 	<ol style="list-style-type: none"> 1. Select a rule on the right pane. 2. Do one of the following: <ul style="list-style-type: none"> • Select a tag in the tag browser and, from the drop-down, 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.

Manage Tags	
<ul style="list-style-type: none"> View the currently selected tags. 	<ol style="list-style-type: none"> Select one or more tags in the tag browser. The tags are filtered using an OR operator. The right pane updates to display the rules that have any of the selected tags. To view the currently selected tags, hover over the Clear label in the tag browser.
<ul style="list-style-type: none"> View rules that match the selected tags. You can filter rules based on tags with an AND or an OR operator. 	<ul style="list-style-type: none"> 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. Repeat to add more tags.  <p>Click the  in the search bar on the right pane. The results are displayed using an AND operator.</p>
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Search for a tag. 	In the tag browser, enter the first few letters of the tag name you want to search for and click  to display the tags that match your input.

Objects > External Dynamic Lists

An [external dynamic list](#) is an address object based on an imported list of IP addresses, URLs, or domain names that can be used in policy rules. You must create this list as a text file and save it to a web server that the firewall can access; the firewall uses the management port to retrieve this list. You can configure the firewall to automatically update the list on a schedule.

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

On each firewall platform, you can configure a maximum of 30 unique sources for external dynamic lists. A source is a URL that includes the IP address or hostname, the path, and the filename for the external dynamic list. The firewall matches the URL (complete string) to determine whether a source is unique.

While the firewall does not impose a limit on the number of lists for a specific type of list, the following limits are enforced:

- IP address—The PA-5000 Series and the PA-7000 Series firewalls support a maximum of 150,000 total IP addresses; all other platforms support a maximum of 50,000 total IP addresses. No limits are enforced for the number of IP addresses per list.
- URLs and domain names—a maximum of 50,000 URLs and 50,000 domains are supported on each platform, with no limits enforced on the number of entries per list.

If you exceed the maximum number of entries that are supported on a platform, the firewall generates a System log and skips the entries that exceed the limit.

The following table describes the external dynamic list settings.

External Dynamic List Setting	Description
Name	Enter a name to identify the external dynamic list (up to 32 characters). This name will appear when selecting the source or destination in a policy.
Shared	Select this option if you want the external dynamic list to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the external dynamic list will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the external dynamic list will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the external dynamic list in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.

External Dynamic List Setting	Description
Type  You cannot mix IP addresses, URLs, and domains names in a single list. Each list must include entries of only one type.	Select from the following types of external dynamic lists: <ul style="list-style-type: none"> IP Address List—Each list can include IP ranges and IP subnets in the IPv4 and IPv6 address space. The list must contain only one IP address, range, or subnet per line. Example: 192.168.80.150/32 2001:db8:123:1::1 or 2001:db8:123:1::/64 192.168.80.0/24 (this indicates all addresses from 192.168.80.0 through 192.168.80.255) 2001:db8:123:1::1 - 2001:db8:123:1::22 A subnet or an IP address range, such as 92.168.20.0/24 or 192.168.20.40-192.168.20.50, count as one IP address entry and not as multiple IP addresses. Domain List—Each list can have only one domain name entry per line. Example: www.p301srv03.paloalonetworks.com ftp.example.co.uk test.domain.net For the list of domains included in the External Dynamic List, the firewall creates a set of custom signatures of type spyware and medium severity, so that you can use the sinkhole action for a custom list of domains. URL List—Each list can have only one URL entry per line. Example: financialtimes.co.in www.wallaby.au/joey www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx *.example.com/* For each URL list, the default action is set to allow. To edit the default action, see Objects > Security Profiles > URL Filtering .
Description	Enter a description for the external dynamic 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.
Frequency	Specify the frequency in which the firewall retrieves the list from the web server. You can choose hourly , five-minute , daily , weekly , or monthly . At the configured interval, the firewall retrieves the list and automatically commits the changes to the configuration. Any policy rules that reference the list are updated so that the firewall can successfully enforce policy.
Test Source URL (Firewall only)	Test that the source URL or server path is available.

Objects > Custom Objects

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

- [Objects > Custom Objects > Data Patterns](#)
- [Objects > Custom Objects > Spyware/Vulnerability](#)
- [Objects > Custom Objects > URL Category](#)

Objects > Custom Objects > Data Patterns

The following topics describe data patterns.

What do you want to know?	See:
Define data patterns.	Data Pattern Settings
Rules for adding data patterns.	Syntax for Data Patterns
Custom data pattern examples.	Data Patterns Examples

Data Pattern Settings

Select **Objects > Custom Objects > Data Patterns** to define the categories of sensitive information that you may want to filter using data filtering security policies. For information on defining data filtering profiles, refer to [Objects > Security Profiles > Data Filtering](#).

The following table describes the data pattern settings.

Data Pattern Setting	Description
Name	Enter the data pattern name (up to 31 characters). The name case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the data pattern (up to 255 characters).
Shared	Select this option if you want the data pattern to be available to: <ul style="list-style-type: none"> • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the data pattern will be available only to the Virtual System selected in the Objects tab. • Every device group on Panorama. If you clear this selection, the data pattern will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the data pattern in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.

Data Pattern Setting	Description
Weight	<p>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.</p> <ul style="list-style-type: none"> • CC#—Specify a weight for the credit card field (range is 0-255). • SSN#—Specify a weight for the social security number field, where the field includes dashes, such as 123-45-6789 (range is 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 is 0-255; 255 is highest weight).
Custom Patterns	<p>The pre-defined patterns include credit card number and social security number (with and without dashes).</p> <p>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. For more information, see Syntax for Data Patterns.</p>

Syntax for 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.

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)*
+	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”—alternative substrings must be in parentheses. Example: ((bif) (scr) (exe)) matches “bif”, “scr”, or “exe”.
-	Used to create range expressions. Example: [c-z] matches any character between c and z, inclusive.

Pattern Rules Syntax	Description
[]	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).
&	& is a special character, so to look for the “&” in a string you must use “&” 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 & Confidential)|(Proprietary and Confidential))
 - Looks for either “Proprietary & Confidential” or “Proprietary and Confidential”
 - More precise than looking for “Confidential”
- .*(Press Release).*((Draft)|(DRAFT)|(draft))
 - Looks for “Press Release” followed by various forms of the word draft, which may indicate that the press release isn’t ready to be sent outside the company
- .*(Trinidad)
 - Looks for a project code name, such as “Trinidad”

Objects > Custom Objects > Spyware/Vulnerability

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



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

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

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

Custom Vulnerability and Spyware Signature Setting	Description
Configuration Tab	
Threat ID	Enter a numeric identifier for the configuration (spyware signatures range is 15000-18000; vulnerability signatures range is 41000-45000).
Name	Specify the threat name.
Shared	Select this option if you want the custom signature to be available to: <ul style="list-style-type: none">Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the custom signature will be available only to the Virtual System selected in the Objects tab.Every device group on Panorama. If you clear this selection, the custom signature will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the signature in descendant device groups by overriding its inherited values. This selection 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.
Default Action	Assign the default action to take if the threat conditions are met. For a list of actions, see Actions in Security Profiles and Custom Objects .
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.

Custom Vulnerability and Spyware Signature Setting	Description
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.

Custom Vulnerability and Spyware Signature Setting	Description
Signatures Tab	
Standard Signature	<p>Select Standard and then Add a new signature. Specify the following information:</p> <ul style="list-style-type: none"> • 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. <p>Add a condition by clicking Add Or Condition or Add And Condition. To add a condition within a group, select the group and then click Add Condition. Add a condition to a signature so that the signature is generated for traffic when the parameters you define for the condition are true. Select an Operator from the drop-down. The operator defines the type of condition that must be true for the custom signature to match to traffic. Choose from Less Than, Equal To, Greater Than, or Pattern Match operators.</p> <ul style="list-style-type: none"> • When choosing a Pattern Match operator, specify for the following to be true for the signature to match to traffic: <ul style="list-style-type: none"> • Context—Select from the available contexts. • Pattern—Specify a regular expression. See Pattern Rules Syntax for pattern rules for regular expressions. • Qualifier and Value—Optionally, add qualifier/value pairs. • Negate—Select Negate so that the custom signature matches to traffic only when the defined Pattern Match condition is not true. This allows you to ensure that the custom signature is not triggered under certain conditions. <p> 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.</p> <p>You can define exceptions for custom vulnerability or spyware signatures using the new option to negate signature generation when traffic matches both a signature and the exception to the signature. Use this option to allow certain traffic in your network that might otherwise be classified as spyware or a vulnerability exploit. In this case, the signature is generated for traffic that matches the pattern; traffic that matches the pattern but also matches the exception to the pattern is excluded from signature generation and any associated policy action (such as being blocked or dropped). For example, you can define a signature to be generated for redirected URLs; however, you can now also create an exception where the signature is not generated for URLs that redirect to a trusted domain.</p>

Custom Vulnerability and Spyware Signature Setting	Description
	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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, 0xfffffff00. Value—Specify a 4-byte hex value, for example, 0xaabbccdd.
Combination Signature	<p>Select Combination and specify the following information:</p> <p>Select Combination Signatures to specify conditions that define signatures:</p> <ul style="list-style-type: none"> Add a condition by clicking Add AND Condition or Add OR Condition. To add a condition within a group, select the group and then click Add Condition. To move a condition within a group, select the condition and click Move Up or Move Down. To move a group, select the group and click Move Up or Move Down. You cannot move conditions from one group to another. <p>Select Time Attribute to specify the following information:</p> <ul style="list-style-type: none"> Number of Hits—Specify the threshold that will trigger any policy-based action as a number of hits (1-1000) in a specified number of seconds (1-3600). Aggregation Criteria—Specify whether the hits are tracked by source IP address, destination IP address, or a combination of source and destination IP addresses. To move a condition within a group, select the condition and click Move Up or Move Down. To move a group, select the group and click Move Up or Move Down. You cannot move conditions from one group to another.

Objects > Custom Objects > URL Category

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



URL entries added to custom categories are case insensitive.

The following table describes the custom URL settings.

Custom URL Category Setting	Description
Name	Enter a name to identify the custom URL category (up to 31 characters). This name displays in the category list when defining URL filtering policies and in the match criteria for URL categories in policy rules. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the URL category (up to 255 characters).
Shared	Select this option if you want the URL category to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the URL category will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the URL category will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from overriding inherited values and creating local copies of the URL category in descendant device groups. This selection is cleared by default, which means overriding is enabled.
Sites	<ul style="list-style-type: none"> Add—Click Add to enter URLs, only one in each row. Each URL can be in the format “www.example.com” or can include wildcards, such as “*.example.com”. For additional information on formats supported, see Block List in Objects > Security Profiles > URL Filtering. Import—Click Import and browse to select the text file that contains the list of URLs. Enter only one URL per row. Each URL can be in the format “www.example.com” or can include wildcards, such as “*.example.com”. For additional information on formats supported, see Block List in Objects > Security Profiles > URL Filtering. Export—Click Export to export the custom URL entries included in the list. The URLs are exported as a text file. Delete—Select an entry and click Delete to remove the URL from the list. <p> To delete a custom category that you have used in a URL filtering profile, you must set the action to None before you can delete the custom category. See Category actions in Objects > Security Profiles > URL Filtering.</p>

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

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

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.

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

Antivirus Profile Setting	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 option if you want the profile to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.
Antivirus tab	
Allows you to specify the action for the different types of traffic, such as ftp, and http.	
Packet Capture	Select this option if you want to capture identified packets.
Decoders and Actions	For each type of traffic that you want to inspect for viruses, select an action from the drop-down. You can define different actions for standard antivirus signatures (Action column) and antivirus signatures that WildFire generates (WildFire Action column). <p>Antivirus content updates are released daily, while WildFire content updates (including antivirus signatures) are released every five minutes as new threats are detected—this means that standard antivirus signatures undergo a longer testing period before release than WildFire antivirus signatures. Because of this, you can choose to enforce different actions for standard antivirus signatures and those generated by WildFire—for example, set alerts for WildFire antivirus signatures instead of blocking them.</p> <p>See Actions in Security Profiles and Custom Objects for a description of each action.</p>

Antivirus Profile Setting	Description
Applications Exceptions and Actions	<p>The Applications Exception table allows you to define applications that will not be inspected. For example, to block all HTTP traffic except for a specific application, you can define an antivirus profile for which the application is an exception. Block is the action for the HTTP decoder, and Allow is the exception for the application. For each application exception, select the action to be taken when the threat is detected. For a list of actions, see Actions in Security Profiles and Custom Objects. 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.</p>
Virus Exception	<p>The Virus Exceptions tab to define a list of threats that will be ignored by the antivirus profile.</p>
Threat ID	<p>To add specific threats that you want to ignore, enter one Threat ID at a time and click Add. Threat IDs are presented as part of the threat log information. Refer to Monitor > Logs.</p>

Objects > Security Profiles > Anti-Spyware Profile

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.

Anti-Spyware Profile Setting	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of Anti-Spyware profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared	Select this option if you want the profile to be available to: <ul style="list-style-type: none"> • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.

Rules

Anti-Spyware rules allow you to define a custom severity and action to take on any threat, a specific threat name that contains the text that you enter, and/or by a threat category, such as adware.

Add a new rule, or you can select an existing rule to and select **Find Matching Signatures** to filter threat signatures based on that rule.

Rule Name	Specify the rule name.
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 and Custom Objects .

Anti-Spyware Profile Setting	Description
Packet Capture	<p>Select this option if you want to capture identified packets.</p> <p>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 provide much more context to the threat when analyzing the threat logs. To view the packet capture, select Monitor > Logs > Threat and locate the log entry you are interested in and then click the green down arrow in the second column. To define the number of packets that should be captured, select Device > Setup > Content-ID and then edit the Content-ID Settings.</p> <p>Packet captures will only occur if the action is allow or alert. If the block action is set, the session is ended immediately.</p>

Exceptions Tab

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

Exceptions	<p>Select Enable for each threat for which you want to assign an action, or select All to respond to all listed threats. The list depends on the selected host, category, and severity. If the list is empty, there are no threats for the current selections.</p> <p>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.</p>
------------	--

DNS Signature Tab

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, sinkhole, or 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.

External Dynamic List Domains	<p>Allows you to select the lists for which you want to enforce an action when a DNS query occurs. By default, the list of DNS signatures provided through content updates (Palo Alto Networks DNS Signatures list) is sinkholed. The default IP address used for sinkholing belongs to Palo Alto Networks (71.19.152.112). This IP address is not static and can be modified through content updates on the firewall or Panorama.</p> <p>To add a new list, click Add and select the External Dynamic List of type Domain that you had created. To create a new list, see Objects > External Dynamic Lists.</p>
-------------------------------	--

Anti-Spyware Profile Setting	Description
Action on DNS queries	<p>Choose an action to be taken when DNS lookups are made to known malware sites. The options are alert, allow, block, or sinkhole. The default action for Palo Alto Networks DNS signatures is sinkhole.</p> <p>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 (such as when 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.</p> <p>After selecting the sinkhole action, specify an IPv4 and/or IPv6 address that will be used for sinkholing. By default, the sinkhole IP address is set to a Palo Alto Networks server. You can then use the traffic logs or build a custom report that filters on the sinkhole IP address and identify infected clients.</p> <p>The following is the sequence of events that will occur when an DNS request is sinkholed:</p> <ul style="list-style-type: none"> • Malicious software on an infected client computer sends a DNS query to resolve a malicious host on the Internet. • The client's DNS query is sent to an internal DNS server, which then queries a public DNS server on the other side of the firewall. • The DNS query matches a DNS entry in the DNS signatures database, so the sinkhole action will be performed on the query. • The infected client then attempts to start a session with the host, but uses the forged IP address instead. The forged IP address is the address defined in the Anti-Spyware profile DNS Signatures tab when the sinkhole action is selected. • The administrator is alerted of a malicious DNS query in the threat log, and can then search the traffic logs for the sinkhole IP address and can easily locate the client IP address that is trying to start a session with the sinkhole IP address.
Packet Capture	Select this option if you want to capture identified packets.

Anti-Spyware Profile Setting	Description
Enable Passive DNS Monitoring	<p>This is 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 (originating from the local recursive resolver—not from 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.</p> <p>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.</p> <p>The option is disabled by default.</p>
Threat ID	Manually enter DNS signature exceptions (range is 4000000-4999999).

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 [Policies > Security](#).

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

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

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

The following tables describe the **Vulnerability Protection profile** settings.

Vulnerability Protection Profile Setting	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 option if you want the profile to be available to: <ul style="list-style-type: none"> • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This selection 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.

Vulnerability Protection Profile Setting	Description
Action	<p>Choose the action to take when the rule is triggered. For a list of actions, see Actions in Security Profiles and Custom Objects.</p> <p>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 be displayed and you will see an Action column.</p>
Host Type	Specify whether to limit the signatures for the rule to those that are client side, server side, or either (any).
Packet Capture	<p>Select this option if you want to capture identified packets.</p> <p>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 provide much more context to the threat when analyzing the threat logs. To view the packet capture, select Monitor > Logs > Threat and locate the log entry you are interested in and then click the green down arrow in the second column. To define the number of packets that should be captured, select Device > Setup > Content-ID and then edit the Content-ID Settings.</p> <p>Packet captures will only occur if the action is allow or alert. If the block action is set, the session is ended immediately.</p>
Category	Select a vulnerability category if you want to limit the signatures to those that match that category.
CVE List	<p>Specify common vulnerabilities and exposures (CVEs) if you want to limit the signatures to those that also match the specified CVEs.</p> <p>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”.</p>
Vendor ID	<p>Specify vendor IDs if you want to limit the signatures to those that also match the specified vendor IDs.</p> <p>For example, the Microsoft vendor IDs are in the form MSyy-xxx, where yy is the two-digit year and xxx is the unique identifier. For example, to match Microsoft for the year 2009, enter “MS09”.</p>
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.

Vulnerability Protection Profile Setting	Description
Exceptions Tab	
Threats	<p>Select Enable for each threat for which you want to assign an action, or select All to respond to all listed threats. The list depends on the selected host, category, and severity. If the list is empty, there are no threats for the current selections.</p> <p>Choose an action from the drop-down, or choose from the Action drop-down at the top of the list to apply the same action to all threats. If you selected Show All, then all signatures are listed. If not, only the signatures that are exceptions are listed.</p> <p>Select Packet Capture if you want to capture identified packets.</p> <p>The vulnerability signature database contains signatures that indicate a brute force attack; for example, Threat ID 40001 triggers on an FTP brute force attack. Brute-force signatures trigger when a condition occurs in a certain time threshold. The thresholds are pre-configured for brute force signatures, and can be changed by clicking edit () next to the threat name on the Vulnerability tab (with the Custom option selected). You can specify the number of hits per unit of time and whether the threshold applies to source, destination, or source-and-destination.</p> <p>Thresholds can be applied on a source IP, destination IP or a combination of source IP and destination IP.</p> <p>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.</p> <p>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.</p>

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 [Policies > Security](#). To create custom URL categories with your own lists of URLs, refer to [Objects > Custom Objects > URL Category](#).

The following tables describe the [URL filtering profile](#) settings.

URL Filtering Profile Setting	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of URL filtering profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared	Select this option if you want the profile to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.
Categories	
Action on License Expiration (Configurable for BrightCloud only)	Select the action to take if the URL filtering license expires: <ul style="list-style-type: none"> Block—Blocks access to all web sites. Allow—Allows access to all web sites.  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: <ul style="list-style-type: none"> 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.

URL Filtering Profile Setting	Description						
<p>Block List</p>  <p>If you would like to use an External Dynamic List to dynamically update (without a commit) the list of URLs that you wish to block, see Objects > External Dynamic Lists.</p>	<p>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.</p>  <p>You must omit the "http and https" portion of the URLs when adding web sites to the list.</p> <p>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".</p> <p>Examples:</p> <ul style="list-style-type: none"> • www.paloaltonetworks.com • 198.133.219.25/en/US <p>Block and allow lists support wildcard patterns. The following characters are considered separators:</p> <ul style="list-style-type: none"> • . • / • ? • & • = • ; • + <p>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:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 30%;"><code>*.yahoo.com</code></td> <td style="width: 70%;"><i>(Tokens are: "*", "yahoo" and "com")</i></td> </tr> <tr> <td><code>www.*.com</code></td> <td><i>(Tokens are: "www", "*" and "com")</i></td> </tr> <tr> <td><code>www.yahoo.com/search=*</code></td> <td><i>(Tokens are: "www", "yahoo", "com", "search", "*")</i></td> </tr> </table> <p>The following patterns are invalid because the character ** is not the only character in the token.</p> <ul style="list-style-type: none"> • <code>ww*.yahoo.com</code> • <code>www.y*.com</code> 	<code>*.yahoo.com</code>	<i>(Tokens are: "*", "yahoo" and "com")</i>	<code>www.*.com</code>	<i>(Tokens are: "www", "*" and "com")</i>	<code>www.yahoo.com/search=*</code>	<i>(Tokens are: "www", "yahoo", "com", "search", "*")</i>
<code>*.yahoo.com</code>	<i>(Tokens are: "*", "yahoo" and "com")</i>						
<code>www.*.com</code>	<i>(Tokens are: "www", "*" and "com")</i>						
<code>www.yahoo.com/search=*</code>	<i>(Tokens are: "www", "yahoo", "com", "search", "*")</i>						
<p>Action</p>	<p>Select the action to take when a web site in the block list is accessed.</p> <ul style="list-style-type: none"> • 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 Device > Setup > Management). 						

URL Filtering Profile Setting	Description
<p>Allow List</p>  If you would like to use an External Dynamic List to dynamically update (without a commit) the list of URLs that you wish to allow, see Objects > External Dynamic Lists	<p>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.</p>  You must omit the "http and https" portion of the URLs when adding web sites to the list.

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:

- | | |
|-------------------------------------|--|
| <code>*.yahoo.com</code> | (Tokens are: "*", "yahoo" and "com") |
| <code>www.*.com</code> | (Tokens are: "www", "*" and "com") |
| <code>www.yahoo.com/search=*</code> | (Tokens are: "www", "yahoo", "com", "search", "*") |

The following patterns are invalid because the character ** is not the only character in the token.

- | |
|----------------------------|
| <code>ww*.yahoo.com</code> |
| <code>www.y*.com</code> |

This list takes precedence over the selected web site categories.

URL Filtering Profile Setting	Description
Category/Action	<p>In addition to the predefined categories, both custom URL categories and external dynamic lists of type URL are displayed under Category. By default, the action for all categories is set to Allow.</p> <p>For each category, select the action to take when a URL in that category is accessed.</p> <ul style="list-style-type: none"> • alert—Allows access to the web site but adds an alert to the URL log each time a user accesses the URL. • allow—Allows access to the web site. • block—Blocks access to the web site. • continue—Displays a response page. To access the web site, the user must click Continue on the response page. • override—Displays a response page that prompts the user to enter a password. The override option restricts access to users with a valid password. Configure URL Admin Override settings (Device > Setup > Content ID) to manage password and other override settings. (See also the Management Settings table in Device > Setup > Content-ID). <p> The Continue and Override pages will not be displayed properly on client machines that are configured to use a proxy server.</p> <ul style="list-style-type: none"> • none (custom URL category only)—If you have created custom URL categories, set the action to none to allow the firewall to inherit the URL filtering category assignment from your URL database vendor. Setting the action to none gives you the flexibility to ignore custom categories in a URL filtering profile, while allowing you to use the custom URL category as a match criteria in policy rules (Security, Decryption, and QoS) to make exceptions or to enforce different actions. To delete a custom URL category, you must set the action to none in any profile where the custom category is used. For information on custom URL categories, see Objects > Custom Objects > URL Category.
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."
Settings	
Log container page only Default: Enabled	Select this option to log only the URLs that match the content type that is specified.

URL Filtering Profile Setting	Description
<p>Enable Safe Search Enforcement Default: Disabled A URL filtering license is not required to use this feature.</p>	<p>Select this option 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.</p> <p> 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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Refer to the PAN-OS 7.1 Administrator's Guide for more information.</p>
HTTP Header Logging	<p>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:</p> <ul style="list-style-type: none"> • 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.

Objects > Security Profiles > File Blocking

A Security policy can include specification of a file blocking profile that blocks selected file types from being uploaded or downloaded, or generates an alert when the specified file types are detected.

To apply file blocking profiles to security policies, refer to [Policies > Security](#).

The following tables describe the [file blocking profile](#) settings.

File Blocking Profile Setting	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of file blocking profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared	Select this option if you want the profile to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This selection 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 : <ul style="list-style-type: none"> Name—Enter a rule name (up to 31 characters). Applications—Select the applications the rule applies to or select any. File Types—Click in the file types field and then click Add to view a list of supported file types. Click a file type to add it to the profile and continue to add additional file types as needed. If you select any, the defined action is taken on all supported file types. Direction—Select the direction of the file transfer (Upload, Download, or Both). Action—Select the action taken when the selected file types are detected: <ul style="list-style-type: none"> 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 , 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.

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).

WildFire Analysis Profile Setting	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 option if you want the profile to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
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. <ul style="list-style-type: none"> 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. Note that a WildFire private cloud (hosted by a WF-500 appliance) does not support analysis for APK files. 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: <ul style="list-style-type: none"> Select public-cloud so that all traffic matched to the rule is forwarded to the WildFire public cloud for analysis. Select private-cloud so that all traffic matched to the rule is forwarded to the WildFire appliance for analysis.

Objects > Security Profiles > Data Filtering

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 [Policies > Security](#).

The following tables describe the [data filtering profile](#) settings.

Data Filtering Profile Setting	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 option if you want the profile to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.
Data Capture	Select this option to automatically collect the data that is blocked by the filter.



Specify a password for Manage Data Protection on the Settings page to view your captured data. Refer to [Device > Setup > Management](#).

To add a data pattern, click **Add** and specify the following information.

Data Pattern Setting	Description
Data Pattern	Choose an existing data pattern from the Data Pattern drop-down or configure a new pattern by choosing Data Pattern from the list and specifying the information described in Objects > Custom Objects > Data Patterns .
Applications	Specify the applications to include in the filtering rule: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.

Data Pattern Setting	Description
Direction	Specify whether to apply the filter in the upload direction, download direction, or both.
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).

Objects > Security Profiles > DoS Protection

DoS Protection profiles are designed for high precision targeting and they augment Zone Protection profiles. A DoS Protection profile specifies the threshold rates of incoming packets and the action the firewall takes to protect against a DoS attack. The profile is attached to DoS Protection policy rule, where you establish the matching criteria for packets that are subject to the Deny, Allow, or Protect action. To attach a DoS Protection profile to a DoS Protection policy rule, see [Policies > DoS 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

The following table describes DoS Protection profile settings.

DoS Protection Profile Setting	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 option if you want the profile to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.
Description	Enter a description of the profile (up to 255 characters).
Type	Select one of the profile types: <ul style="list-style-type: none"> 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 profile with a SYN flood threshold of 10,000 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 that match the classification criterion (source IP, destination IP or source-and-destination IP).

DoS Protection Profile Setting	Description
Flood Protection Tab	
Syn Flood tab UDP Flood tab ICMP Flood tab ICMPv6 tab Other IP tab	<p>Select this option to enable the type of flood protection indicated on the tab, and specify the following settings:</p> <ul style="list-style-type: none"> • Action—(SYN Flood only) Action that the firewall performs if the DoS Protection policy action is Protect and if the Activate Rate threshold is reached. Choose one of the following: <ul style="list-style-type: none"> • Random Early Drop—Drop packets randomly when the Activate Rate threshold is reached. • SYN cookies—Use SYN cookies to generate acknowledgments so that it is not necessary to drop connections during a SYN flood attack. • Alarm Rate—Specify the threshold rate (pps) at which a DoS alarm is generated (range is 0-2,000,000 pps; default is 10,000 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 Protection profile (Random Early Drop or SYN cookies). The Activate Rate range is 0-2,000,000 pps; default is 10,000 pps). If the profile Action is Random Early Drop (RED), when the Activate Rate threshold is reached, RED occurs. If the incoming packet rate increases, the RED rate increases according to an algorithm. The firewall continues to do Random Early Drop until the packet rate reaches the Max Rate threshold. At the Max Rate threshold, the firewall drops 100% of incoming packets. • 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. (Range is 2-2,000,000 pps; default is 40,000 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 1-21,600; default is 300.) <p>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.</p>
Resources Protection Tab	
Sessions	Select this option to enable Resources Protection.
Max Concurrent Limit	<p>Specify the maximum number of concurrent sessions.</p> <ul style="list-style-type: none"> • If the DoS Protection profile type is Aggregate, this limit applies to all traffic hitting the DoS Protection rule on which the DoS Protection profile is applied. • If the DoS Protection profile type is Classified, this limit applies to the traffic on a classified basis (source IP, destination IP or source-and-destination IP) hitting the DoS Protection rule on which the DoS Protection profile is applied.

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

The following table describes the Security Profile settings.

Security Profile Group Setting	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 option if you want the profile group to be available to: <ul style="list-style-type: none">• Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile group will be available only to the Virtual System selected in the Objects tab.• Every device group on Panorama. If you clear this selection, the profile group will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile group in descendant device groups by overriding its inherited values. This selection 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 Objects > Security Profiles > Data Filtering .

Objects > Log Forwarding

Each Security policy can specify a log forwarding profile that determines whether traffic, threat, and WildFire Submissions log entries are logged remotely with Panorama, and/or sent as SNMP traps, syslog messages, or email notifications:

- Traffic logs record information about each traffic flow.
- 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).
- WildFire Submissions logs record the files and email links that the firewall forwards for WildFire analysis, including the WildFire verdict for each sample (benign, grayware, or malicious).

By default, the firewall performs local logging. To enable a log forwarding profile, attach it to a [Policies > Security](#) rule.



On a PA-7000 Series firewalls, you must configure a [Log Card Interface](#) 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.

PA-7000 Series firewalls cannot forward logs to Panorama, only to external services. However, when you use Panorama to monitor logs or generate reports for a device group that includes a PA-7000 Series firewall, Panorama queries the firewall in real-time to display its log data.

The following table describes the log forwarding settings.

Log Forwarding Profile Setting	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 option if you want the profile to be available to: <ul style="list-style-type: none"> • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. • Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.
Traffic Settings	
Panorama	Select this option to enable sending traffic log entries to the Panorama centralized management system. To define the Panorama server address, refer to Device > Setup > Management .

Log Forwarding Profile Setting	Description
SNMP Trap Email Syslog	<p>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:</p> <ul style="list-style-type: none"> • Device > Server Profiles > SNMP Trap • Device > Server Profiles > Email • Device > Server Profiles > Syslog
Threat Settings	
Panorama	<p>Click this option for each severity level of the threat log entries to be sent to Panorama. The severity levels are:</p> <ul style="list-style-type: none"> • 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	<p>Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the threat log entries are sent. To define new destinations, refer to:</p> <ul style="list-style-type: none"> • Device > Server Profiles > SNMP Trap • Device > Server Profiles > Email • Device > Server Profiles > Syslog
WildFire Settings	
Panorama	<p>Enable the firewall to forward WildFire Submissions log entries to Panorama, based on the WildFire verdict of the submitted file or email link.</p>
SNMP Trap Email Syslog	<p>For each WildFire verdict, select the SNMP, syslog, and/or email settings to specify destinations to send WildFire Submissions logs. To define new destinations, refer to:</p> <ul style="list-style-type: none"> • Device > Server Profiles > SNMP Trap • Device > Server Profiles > Email • Device > Server Profiles > Syslog

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 firewall trusts. For more information, refer to [Manage 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.

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

Decryption Profile General Settings

The following table describes the general settings for decryption profiles.

Decryption Profile — General Setting	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 option if you want the profile to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the profile will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This selection is cleared by default, which means overriding is enabled.

Decryption Profile – General Setting	Description
Decryption Mirroring Interface (PA-3000 Series, PA-5000 Series, and PA-7000 Series firewalls only)	Select an Interface to use for decryption port mirroring.  Before you can enable decryption port mirroring, you must obtain a Decryption Port Mirror license, install the license, and reboot the firewall.
Forwarded Only (PA-3000 Series, PA-5000 Series, and PA-7000 Series firewalls only)	Select Forwarded Only if you want to mirror decrypted traffic only after Security policy enforcement. With this option, only traffic that is forwarded through the firewall is mirrored. This option is useful if you are forwarding the decrypted traffic to other threat detection devices, such as a DLP device or another intrusion prevention system (IPS). If you clear this selection (the default setting), the firewall will mirror all decrypted traffic to the interface before security policies lookup, which allows you to replay events and analyze traffic that generates a threat or triggers a drop action.

Settings to Control Decrypted SSL Traffic

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.

SSL Decryption Tab Setting	Description
SSL Forward Proxy Tab 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.

SSL Decryption Tab Setting	Description
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.



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

SSL Inbound Inspection Tab

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

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 Tab

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.
Key Exchange Algorithms	Enforce the use of the selected key exchange algorithms for the SSL session. To implement Perfect Forward Secrecy (PFS) for SSL Forward Proxy decrypted traffic, you can select DHE to enable Diffie-Hellman key exchange based PFS or ECDHE to enable elliptic curve Diffie-Hellman-based PFS.
Encryption Algorithms	Enforce the use of the selected encryption algorithms for the SSL session.

SSL Decryption Tab Setting	Description
Authentication Algorithms	Enforce the use of the selected authentication algorithms for the SSL session.

Settings to Control Traffic that is not Decrypted

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

No Decryption Tab Setting	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.

Settings to Control Decrypted SSH Traffic

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

SSH Proxy Tab Setting	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.

Objects > Schedules

▲ Objects > Schedules

By default, Security policy rules are always in effect (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 [Policies > Security](#).



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 schedule settings.

Schedule Setting	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 option if you want the schedule to be available to: <ul style="list-style-type: none"> Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the schedule will be available only to the Virtual System selected in the Objects tab. Every device group on Panorama. If you clear this selection, the schedule will be available only to the Device Group selected in the Objects tab.
Disable override (Panorama only)	Select this option if you want to prevent administrators from creating local copies of the schedule in descendant device groups by overriding its inherited values. This selection 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	Add and specify a start and end date and time.



Network

- ▲ [Network > Virtual Wires](#)
- ▲ [Network > Interfaces](#)
- ▲ [Network > Virtual Routers](#)
- ▲ [Network > Zones](#)
- ▲ [Network > VLANs](#)
- ▲ [Network > IPSec Tunnels](#)
- ▲ [Network > DHCP](#)
- ▲ [Network > DNS Proxy](#)
- ▲ [Network > QoS](#)
- ▲ [Network > LLDP](#)
- ▲ [Network > Network Profiles](#)

Network > Virtual Wires

Select **Network > Virtual Wires** to define virtual wires after you have specified two virtual wire interfaces on the firewall.

Virtual Wire Setting	Description
Virtual Wire Name	Enter a virtual wire name (up to 31 characters). This name appears in the list of virtual wires when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Interfaces	Select two Ethernet interfaces from the displayed list for the virtual wire configuration. Interfaces are listed here only if they have the virtual wire interface type and have not been assigned to another virtual wire. For information on virtual wire interfaces, see Virtual Wire Interface .
Tag Allowed	Enter the tag number (0-4,094) 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 option if you want to bring down the other port in a virtual wire when a down link state is detected. If you do not select or you disable this option, link status is not propagated across the virtual wire.

Network > Interfaces

Firewall interfaces (ports) enable a firewall to connect with other network devices and with other interfaces within the firewall. The following topics describe the interface types and how to configure them.

What do you want to know?	See:
What are firewall interfaces?	Firewall Interfaces Overview
I am new to firewall interfaces; what are the components of a firewall interface?	Common Building Blocks for Firewall Interfaces Common Building Blocks for PA-7000 Series Firewall Interfaces
I already understand firewall interfaces; how can I find information on configuring a specific interface type?	<p>Physical Interfaces (Ethernet)</p> <ul style="list-style-type: none">• Layer 2 Interface• Layer 2 Subinterface• Layer 3 Interface• Layer 3 Subinterface• Virtual Wire Interface• Virtual Wire Subinterface• Tap Interface• Log Card Interface• Log Card Subinterface• Decrypt Mirror Interface• Aggregate Ethernet (AE) Interface Group• Aggregate Ethernet (AE) Interface• HA Interface <p>Logical Interfaces</p> <ul style="list-style-type: none">• Network > Interfaces > VLAN• Network > Interfaces > Loopback• Network > Interfaces > Tunnel
Looking for more?	Networking

Firewall Interfaces Overview

The interface configurations of firewall data ports enable traffic to enter and exit the firewall. A Palo Alto Networks firewall can operate in multiple deployments simultaneously because you can configure 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 supports two kinds of Ethernet—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

Select **Network > Interfaces** to display and configure the components that are common to most interface types.



For a description of components that are unique or different when you configure interfaces on a PA-7000 Series firewall, or when you use Panorama™ to configure interfaces on any firewall, see [Common Building Blocks for PA-7000 Series Firewall Interfaces](#).

Firewall Interface Building Block	Description
Interface (Interface Name)	The interface name is predefined and you cannot change it. However, you can append a numeric suffix for subinterfaces, aggregate interfaces, VLAN interfaces, loopback interfaces, and tunnel interfaces.
Interface Type	For Ethernet interfaces (Network > Interfaces > Ethernet), you can select the interface type: <ul style="list-style-type: none"> • 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 Management Profile (Network > Interfaces > <if-config> Advanced > Other Info) that defines the protocols (such as SSH, Telnet, and HTTP) you can use to manage the firewall over this interface.

Firewall Interface Building Block	Description
Link State	<p>For Ethernet interfaces, Link State indicates whether the interface is currently accessible and can receive traffic over the network:</p> <ul style="list-style-type: none"> • Green—Configured and up • Red—Configured but down or disabled • Gray—Not configured <p>Hover over the link state to display a tool tip that indicates the link speed and duplex settings for that interface.</p>
IP Address	<p>(Optional) Configure the IPv4 or IPv6 address of the Ethernet, VLAN, loopback, or tunnel interface. For an IPv4 address, you can also select the addressing mode (Type) for the interface—Static, DHCP Client, or PPPoE.</p>
Virtual Router	<p>Assign a virtual router to the interface or click Virtual Router to define a new one (see Network > Virtual Routers). Select None to remove the current virtual router assignment from the interface.</p>
Tag (Subinterface only)	<p>Enter the VLAN tag (1-4,094) for the subinterface.</p>
VLAN	<p>Select Network > Interfaces > VLAN and modify an existing VLAN or Add a new one (see Network > VLANs). Select None to remove the current VLAN assignment from the interface. To enable switching between Layer 2 interfaces, or to enable routing through a VLAN interface, you must configure a VLAN object.</p>
Virtual System	<p>If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click Virtual System to define a new vsys.</p>
Security Zone	<p>Select a Security Zone (Network > Interfaces > <if-config> > Config) for the interface, or select Zone to define a new one. Select None to remove the current zone assignment from the interface.</p>
Features	<p>For Ethernet interfaces, this column indicates whether the following features are enabled:</p> <ul style="list-style-type: none"> • —GlobalProtect gateway • —Link Aggregation Control Protocol (LACP) • —Quality of Service (QoS) profile • —Link Layer Discovery Protocol (LLDP) • —NetFlow profile • —Dynamic Host Configuration Protocol (DHCP) client—The interface acts as a DHCP client and receives a dynamically assigned IP address.
Comment	<p>A description of the interface function or purpose.</p>

Common Building Blocks for PA-7000 Series Firewall Interfaces

The following table describes the components of the **Network > Interfaces > Ethernet** page that are unique or different when you configure interfaces on a PA-7000 Series firewall, or when you use Panorama to configure interfaces on any firewall. Click **Add Interface** to create a new interface or select an existing interface (ethernet1/1, for example) to edit it.



On PA-7000 Series firewalls, if you configure log forwarding on the firewall, you must configure one data port as a [Log Card Interface](#).

PA-7000 Series Firewall Interface Building Block	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 .

Layer 2 Interface

▲ Network > Interfaces > Ethernet

Select **Network > Interfaces > Ethernet** to configure a Layer 2 interface. click the name of an Interface (ethernet1/1, for example) that is not configured and specify the following information.

Layer 2 Interface Setting	Configured In	Description
Interface Name	Ethernet Interface	The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select Layer2 .
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Select None to remove the current NetFlow server assignment from the interface.  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 an existing VLAN or click VLAN to define a new VLAN (see Network > VLANs). Select None to remove the current VLAN assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system for the interface or click Virtual System to define a new vsys.
Security Zone		Select a Security Zone for the interface or click Zone to define a new zone. Select None to remove the current zone assignment from the interface.
Link Speed	Ethernet Interface > Advanced	Select the interface speed in Mbps (10 , 100 , or 1000) or select auto to have the firewall automatically determine the speed.
Link Duplex		Select whether the interface transmission mode is full-duplex (full), half-duplex (half), or negotiated automatically (auto).
Link State		Select whether the interface status is enabled (up), disabled (down), or determined automatically (auto).
Enable LLDP	Ethernet Interface > Advanced > LLDP	Select 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		If LLDP is enabled, select an LLDP profile to assign to the interface or click LLDP Profile to create a new profile (see Network > Network Profiles > LLDP Profile). Select None to configure the firewall to use global defaults.
Enable in HA Passive State		If LLDP is enabled, select this option to allow an HA passive firewall to pre-negotiate LLDP with its peer before the firewall becomes active.

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 Interface](#), select the row of that physical Interface, click **Add Subinterface**, and specify the following information.

Layer 2 Subinterface Setting	Description
Interface Name	The read-only Interface Name displays the name of the physical interface you selected. In the adjacent field, enter a numeric suffix (1-9,999) to identify the subinterface.
Comment	Enter an optional description for the subinterface.
Tag	Enter the VLAN tag (1-4,094) for the subinterface.
Netflow Profile	If you want to export unidirectional IP traffic that traverses an ingress subinterface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Select None to remove the current NetFlow server assignment from the subinterface.  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 VLAN to define a new VLAN (see Network > VLANs). Select None to remove the current VLAN assignment from the subinterface.
Virtual System	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the subinterface or click Virtual System to define a new vsys.
Security Zone	Select a security zone for the subinterface or click Zone to define a new zone. Select None to remove the current zone assignment from the subinterface.

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.

Layer 3 Interface Setting	Configured In	Description
Interface Name	Ethernet Interface	The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select Layer3 .
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Select None to remove the current NetFlow server assignment from the interface.  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 Virtual Router to define a new one (see Network > Virtual Routers). Select None to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click Virtual System to define a new vsys.
Security Zone		Select a security zone for the interface or click Zone to define a new zone. Select None to remove the current zone assignment from the interface.
Link Speed	Ethernet Interface > Advanced	Select the interface speed in Mbps (10 , 100 , or 1000) or select auto .
Link Duplex		Select whether the interface transmission mode is full-duplex (full), half-duplex (half), or negotiated automatically (auto).
Link State		Select whether the interface status is enabled (up), disabled (down), or determined automatically (auto).

Layer 3 Interface Setting	Configured In	Description
Management Profile	Ethernet Interface > Advanced > Other Info	Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select None to remove the current profile assignment from the interface.
MTU		Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an ICMP fragmentation needed message to the source indicating the packet is too large.
Adjust TCP MSS		Select this option to adjust the maximum segment size (MSS) to accommodate bytes for any headers within the interface MTU byte size. The MTU byte size minus the MSS Adjustment Size equals the MSS byte size, which varies by IP protocol: <ul style="list-style-type: none"> • IPv4 MSS Adjustment Size—Range is 40-300; default is 40. • IPv6 MSS Adjustment Size—Range is 60-300; default is 60. Use these settings to address the case where a tunnel through the network requires a smaller MSS. If a packet has more bytes than the MSS without fragmentation, this setting enables the adjustment. Encapsulation adds length to headers so it is helpful to configure the MSS adjustment size to allow bytes for such things as an MPLS header or tunneled traffic that has a VLAN tag.
Untagged Subinterface		Specifies that all subinterfaces belonging to this Layer 3 interface are untagged. PAN-OS® selects an untagged subinterface as the ingress interface based on the packet destination. If the destination is the IP address of an untagged subinterface, it maps to the subinterface. This also means that packets in the reverse direction must have their source address translated to the IP address of the untagged subinterface. A byproduct of this classification mechanism is that all multicast and broadcast packets are assigned to the base interface, not any subinterfaces. Because Open Shortest Path First (OSPF) uses multicast, the firewall does not support it on untagged subinterfaces.
IP Address MAC Address	Ethernet Interface > Advanced > ARP Entries	To add one or more static Address Resolution Protocol (ARP) entries, click Add and enter an IP address and its associated hardware (MAC) address. To delete an entry, select the entry and click Delete . Static ARP entries reduce ARP processing and preclude man-in-the-middle attacks for the specified addresses.
IPv6 Address MAC Address	Ethernet Interface > Advanced > ND Entries	To provide neighbor information for Neighbor Discovery Protocol (NDP), click Add and enter the IP address and MAC address of the neighbor.

Layer 3 Interface Setting	Configured In	Description
Enable NDP Proxy	Ethernet Interface > Advanced > NDP Proxy	Select this option to enable the Neighbor Discovery Protocol (NDP) proxy for the interface. The firewall will respond to ND packets requesting MAC addresses for IPv6 addresses in this list. In the ND response, the firewall sends its own MAC address for the interface to indicate it will act as proxy by responding to packets destined for those addresses. It is recommended that you select Enable NDP Proxy if you use Network Prefix Translation IPv6 (NPTv6). If Enable NDP Proxy is selected, you can filter numerous Address entries by entering a search string and clicking Apply Filter ().
Address		Click Add to enter one or more IPv6 addresses, IP ranges, IPv6 subnets, or address objects for which the firewall will act as the NDP proxy. Ideally, one of these addresses is the same address as that of the source translation in NPTv6. The order of addresses does not matter. If the address is a subnetwork, the firewall will send an ND response for all addresses in the subnet, so we recommend that you also add the IPv6 neighbors of the firewall and then select Negate to instruct the firewall not to respond to these IP addresses.
Negate		Select Negate for an address to prevent NDP proxy for that address. You can negate a subset of the specified IP address range or IP subnet.
Enable LLDP	Ethernet Interface > Advanced > LLDP	Select to enable Link Layer Discovery Protocol (LLDP) on the interface. LLDP functions at the link layer to discover neighboring devices and their capabilities.
LLDP Profile		If LLDP is enabled, select an LLDP profile to assign to the interface or click LLDP Profile to create a new profile (see Network > Network Profiles > LLDP Profile). Select None to configure the firewall to use global defaults.
Enable in HA Passive State		If LLDP is enabled, select this option to allow the firewall as an HA passive firewall to pre-negotiate LLDP with its peer before the firewall becomes active.
For an IPv4 address		
Type	Ethernet Interface > IPv4	Select the method for assigning an IPv4 address type to the interface: <ul style="list-style-type: none"> Static—You must manually specify the IP address. PPPoE—The firewall will use the interface for Point-to-Point Protocol over Ethernet (PPPoE). DHCP Client—Enables the interface to act as a Dynamic Host Configuration Protocol (DHCP) client and receive a dynamically assigned IP address.  Firewalls that are in 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.

Layer 3 Interface Setting	Configured In	Description
• IPv4 address Type = Static		
IP	Ethernet Interface > IPv4	<p>Click Add, then perform one of the following steps to specify a static IP address and network mask for the interface.</p> <ul style="list-style-type: none"> Type the entry in Classless Inter-domain Routing (CIDR) notation using the format <i>ip_address/mask</i>. IPv4 example: 192.168.2.0/24 IPv6 example: 2001:db8::/32 Select an existing address object of type IP netmask. Click Address to create an address object of type IP netmask. <p>You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your firewall uses determines the maximum number of IP addresses.</p> <p>To delete an IP address, select the address and click Delete.</p>
• IPv4 address Type = PPPoE		
Enable	Ethernet Interface > IPv4 > PPPoE > General	Select this option to activate the interface for PPPoE termination.
Username		Enter the user name for the point-to-point connection.
Password/Confirm Password		Enter and then confirm the password for the user name.
Show PPPoE Client Runtime Info		(Optional) Opens a dialog that displays parameters that the firewall negotiated with the Internet service provider (ISP) to establish a connection. The specific information depends on the ISP.

Layer 3 Interface Setting	Configured In	Description
Authentication	Ethernet Interface > IPv4 > PPPoE > Advanced	Select the authentication protocol for PPPoE communications— CHAP (Challenge-Handshake Authentication Protocol), PAP (Password Authentication Protocol), or the default Auto (the firewall determines the protocol). Select None to remove the current protocol assignment from the interface.
Static Address		<p>Perform one of the following steps to specify the IP address that the Internet service provider assigned (no default value):</p> <ul style="list-style-type: none"> Type the entry in Classless Inter-domain Routing (CIDR) notation using the format <i>ip_address/mask</i>. IPv4 example: 192.168.2.0/24 IPv6 example: 2001:db8::/32 Select an existing address object of type IP netmask. Click Address to create an address object of type IP netmask. Select None to remove the current address assignment from the interface.
Automatically create default route pointing to peer		Select this option to automatically create a default route that points to the PPPoE peer when connected.
Default Route Metric		(Optional) For the route between the firewall and Internet service provider, enter a route metric (priority level) to associate with the default route and to use for path selection (range is 1-65,535). The priority level increases as the numeric value decreases.
Access Concentrator		(Optional) Enter the name of the access concentrator on the Internet service provider end to which the firewall connects (no default).
Service		(Optional) Enter the service string (no default).
Passive		Select this option to use passive mode. In passive mode, a PPPoE endpoint waits for the access concentrator to send the first frame.
<ul style="list-style-type: none"> IPv4 address Type = DHCP 		
Enable	Ethernet Interface > IPv4	Activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server		Automatically create a default route that points to the default gateway that the DHCP server provides.
Default Route Metric		For the route between the firewall and DHCP server, optionally enter a route metric (priority level) to associate with the default route and to use for path selection (range is 1-65,535, no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info		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).

Layer 3 Interface Setting	Configured In	Description
For an IPv6 address		
Enable IPv6 on the interface	Ethernet Interface > IPv6	Enable IPv6 addressing on this interface.
Interface ID		Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the Use interface ID as host portion option when adding an address, the firewall uses the interface ID as the host portion of that address.
Address		<p>Add one or more IPv6 address and configure the following settings:</p> <ul style="list-style-type: none"> • Address—Enter an IPv6 address and prefix length (such as 2001:400:f00::1/64). You can also select an existing IPv6 address object or click Address to create an address object. • Enable address on interface—Select to enable the IPv6 address on the interface. • Use interface ID as host portion—Select to use the Interface ID as the host portion of the IPv6 address. • Anycast—Select to include routing through the nearest node. • Send Router Advertisement—Select this option 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. <p>The remaining fields only apply if you enable RA.</p> <ul style="list-style-type: none"> – Valid Lifetime—The length of time (in seconds) that the firewall considers the address as valid. The valid lifetime must equal or exceed the Preferred Lifetime. The default is 2,592,000. – Preferred Lifetime—The length of time (in seconds) that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new connections but any existing connections are valid until the Valid Lifetime expires. The default is 604,800. – On-link—Select this option if systems that have addresses within the prefix are reachable without a router. – Autonomous—Select if systems can independently create an IP address by combining the advertised prefix with an interface ID.
Enable Duplication Address Detection		Select to enable duplicate address detection (DAD), then configure the other fields in this section.
DAD Attempts		Specify the number of DAD attempts within the neighbor solicitation interval (NS Interval) before the attempt to identify neighbors fails (range is 1-10; default is 1).
Reachable Time		Specify the length of time (in seconds) that a neighbor remains reachable after a successful query and response (range is 10-36,000; default is 30).
NS Interval (neighbor solicitation interval)		Specify the number of seconds for DAD attempts before failure is indicated (range is 1-10; default is 1).

Layer 3 Interface Setting	Configured In	Description
Enable Router Advertisement	Ethernet Interface > IPv6 (cont)	To provide stateless address auto-configuration (SLAAC) on IPv6 interfaces, select and configure this option. Clients that receive the router advertisement (RA) messages use this information. RA enables the firewall to act as a default gateway for IPv6 hosts that are not statically configured and to provide the host with an IPv6 prefix for address configuration. You can use a separate DHCPv6 server in conjunction with this feature to provide DNS and other settings to clients. This is a global setting for the interface. If you want to set RA options for individual IP addresses, Add and configure the address in the IP address table. If you set RA options for any IP address, you must select the Enable Router Advertisement option for the interface.
Min Interval (sec)		Specify the minimum interval (in seconds) between RAs that the firewall will send (range is 3-1,350; default is 200). The firewall will send RAs at random intervals between the minimum and maximum values.
Max Interval (sec)		Specify the maximum interval (in seconds) between RAs that the firewall will send (range is 4-1,800; default is 600). The firewall will send RAs at random intervals between the minimum and maximum values.
Hop Limit		Specify the hop limit to apply to clients for outgoing packets (range is 1-255; default is 64). Enter 0 for no hop limit.
Link MTU		Specify link maximum transmission unit (MTU) to apply to clients. Select unspecified for no link MTU (range is 1,280-9,192; default is unspecified).
Reachable Time (ms)		Specify the reachable time (in milliseconds) that the client will use to assume a neighbor is reachable after receiving a reachability confirmation message. Select unspecified for no reachable time value (range is 0-3,600,000; default is unspecified).
Retrans Time (ms)		Specify the retransmission timer that determines how long the client will wait (in milliseconds) before retransmitting neighbor solicitation messages. Select unspecified for no retransmission time (range is 0-4,294,967,295; default is unspecified).
Router Lifetime (sec)		Specify how long (in seconds) the client will use the firewall as the default gateway (range is 0-9,000; default is 1,800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
Router Preference		If the network segment has multiple IPv6 routers, the client uses this field to select a preferred router. Select whether the RA advertises the firewall router as having a High , Medium (default), or Low priority relative to other routers on the segment.
Managed Configuration		Indicate to the client that addresses are available via DHCPv6.
Other Configuration		Select this option to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check		Select this option 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.

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 Interface](#), select the row of that physical Interface, click **Add Subinterface**, and specify the following information.

Layer 3 Subinterface Setting	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 (1-9,999) to identify the subinterface.
Comment		Enter an optional description for the subinterface.
Tag		Enter the VLAN tag (1-4,094) for the subinterface.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress subinterface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Select None to remove the current NetFlow server assignment from the subinterface.  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 Virtual Router to define a new one (see Network > Virtual Routers). Select None to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the subinterface or click Virtual System to define a new vsys.
Security Zone		Select a security zone for the subinterface, or click Zone to define a new zone. Select None to remove the current zone assignment from the subinterface.

Layer 3 Subinterface Setting	Configured In	Description
Management Profile	Layer3 Subinterface > Advanced > Other Info	Management Profile —Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select None to remove the current profile assignment from the interface.
MTU		Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an ICMP fragmentation needed message to the source indicating the packet is too large.
Adjust TCP MSS		Select this option to adjust the maximum segment size (MSS) to accommodate bytes for any headers within the interface MTU byte size. The MTU byte size minus the MSS Adjustment Size equals the MSS byte size, which varies by IP protocol: <ul style="list-style-type: none"> • IPv4 MSS Adjustment Size—Range is 40-300; default is 40. • IPv6 MSS Adjustment Size—Range is 60-300; default is 60. Use these settings to address the case where a tunnel through the network requires a smaller MSS. If a packet has more bytes than the MSS without fragmentation, this setting enables the adjustment. Encapsulation adds length to headers so it helps to configure the MSS adjustment size to allow bytes for such things as an MPLS header or tunneled traffic that has a VLAN tag.
IP Address MAC Address	Layer3 Subinterface > Advanced > ARP Entries	To add one or more static Address Resolution Protocol (ARP) entries, Add an IP address and its associated hardware (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), Add the IP address and MAC address of the neighbor.

Layer 3 Subinterface Setting	Configured In	Description
Enable NDP Proxy	Layer3 Subinterface > Advanced > NDP Proxy	<p>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.</p> <p>It is recommended that you enable NDP proxy if you are using Network Prefix Translation IPv6 (NPTv6).</p> <p>If you selected Enable NDP Proxy, you can filter numerous Address entries by entering a filter and clicking Apply Filter (gray arrow).</p>
Address		<p>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.</p> <p>If the address is a subnetwork, the firewall will send an ND response for all addresses in the subnet, so we recommend you also add the IPv6 neighbors of the firewall and then click Negate to instruct the firewall not to respond to these IP addresses.</p>
Negate		Select Negate for an address to prevent NDP proxy for that address. You can negate a subset of the specified IP address range or IP subnet.
For an IPv4 address		
Type	Layer3 Subinterface > IPv4	<p>Select the method for assigning an IPv4 address type to the subinterface:</p> <ul style="list-style-type: none"> 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. <p> Firewalls that are in active/active high availability (HA) mode don't support DHCP Client.</p> <p>Based on your IP address method selection, the options displayed in the tab will vary.</p>
<ul style="list-style-type: none"> IPv4 address Type = Static 		
IP	Layer3 Subinterface > IPv4	<p>Click Add, then perform one of the following steps to specify a static IP address and network mask for the interface.</p> <ul style="list-style-type: none"> Type the entry in Classless Inter-domain Routing (CIDR) notation using the format <i>ip_address/mask</i>. IPv4 example: 192.168.2.0/24 IPv6 example: 2001:db8::/32 Select an existing address object of type IP netmask. Click Address to create an address object of type IP netmask. <p>You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses.</p> <p>To delete an IP address, select the address and click Delete.</p>

Layer 3 Subinterface Setting	Configured In	Description
<ul style="list-style-type: none"> IPv4 address Type = DHCP 		
Enable	Layer3 Subinterface > IPv4	Select this option to activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server		Select this option to automatically create a default route that points to the default gateway that the DHCP server provides.
Default Route Metric		(Optional) For the route between the firewall and DHCP server, you can enter a route metric (priority level) to associate with the default route and to use for path selection (range is 1-65535; there is no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info		Select Show DHCP Client Runtime Info to display all settings received from the DHCP server, including DHCP lease status, dynamic IP address assignment, subnet mask, gateway, and server settings (DNS, NTP, domain, WINS, NIS, POP3, and SMTP).
For an IPv6 address		
Enable IPv6 on the interface	Layer3 Subinterface > IPv6	Select this option to enable IPv6 addressing on this interface.
Interface ID		Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the Use interface ID as host portion option when adding an address, the firewall uses the interface ID as the host portion of that address.

Layer 3 Subinterface Setting	Configured In	Description
Address	Layer3 Subinterface > IPv6 (cont)	<p>Click Add and configure the following parameters for each IPv6 address:</p> <ul style="list-style-type: none"> • Address—Enter an IPv6 address and prefix length (e.g. 2001:400:f00::1/64). You can also select an existing IPv6 address object or click Address to create an address object. • Enable address on interface—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. <p>The remaining fields apply only if you enable RA.</p> <ul style="list-style-type: none"> • Valid Lifetime—The length of time (in seconds) that the firewall considers the address as valid. The valid lifetime must equal or exceed the Preferred Lifetime. The default is 2,592,000. • Preferred Lifetime—The length of time (in seconds) that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new connections but any existing connections are valid until the Valid Lifetime expires. The default is 604,800. • 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		Select this option to enable duplicate address detection (DAD), then configure the other fields in this section.
DAD Attempts		Specify the number of DAD attempts within the neighbor solicitation interval (NS Interval) before the attempt to identify neighbors fails (range is 1-10; default is 1).
Reachable Time		Specify the length of time (in seconds) that a neighbor remains reachable after a successful query and response (range is 1-36,000; default is 30).
NS Interval (neighbor solicitation interval)		Specify the number of seconds for DAD attempts before failure is indicated (range is 1-10; default is 1).

Layer 3 Subinterface Setting	Configured In	Description
Enable Router Advertisement	Layer3 Subinterface > IPv6 (cont)	To provide stateless address auto-configuration (SLAAC) on IPv6 interfaces, select this option and configure associated settings. 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. If you set RA options for any IP address, you must select the Enable Router Advertisement option for the interface.
Min Interval (sec)		Specify minimum interval (in seconds) between RAs the firewall will send (range is 3-1,350; default is 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)		Specify the maximum interval (in seconds) between RAs the firewall will send (range is 4-1,800; default is 600). The firewall will send RAs at random intervals between minimum and maximum values you configure.
Hop Limit		Specify the hop limit to apply to clients for outgoing packets (range is 1-255; default is 64). Enter 0 for no hop limit.
Link MTU		Specify link maximum transmission unit (MTU) to apply to clients. Select unspecified for no link MTU (range is 1,280-9,192; default is unspecified).
Reachable Time (ms)		Specify the reachable time (in milliseconds) that the client will use to assume a neighbor is reachable after receiving a reachability confirmation message. Select unspecified for no reachable time value (range is 0-3,600,000; default is unspecified).
Retrans Time (ms)		Specify the retransmission timer that determines how long the client will wait (in milliseconds) before retransmitting neighbor solicitation messages. Select unspecified for no retransmission time (range is 0-4,294,967,295; default is unspecified).
Router Lifetime (sec)		Specify how long (in seconds) the client will use the firewall as the default gateway (range is 0-9,000; default is 1,800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
Router Preference		If the network segment has multiple IPv6 routers, the client uses this field to select a preferred router. Select whether the RA advertises the firewall router as having a High , Medium (default), or Low priority relative to other routers on the segment.
Managed Configuration		Select to indicate to the client that addresses are available via DHCPv6.
Other Configuration		Select this option to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check		Select this option 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.

Virtual Wire Interface

▲ Network > Interfaces > Ethernet

A virtual wire logically binds two Ethernet interfaces together, allowing for all traffic to pass between the interfaces, or just traffic with selected VLAN tags (no other switching or routing services are available). You can create virtual wire subinterfaces to classify traffic according to an IP address, IP range, or subnet. A virtual wire requires no changes to adjacent network devices. A virtual wire can bind two Ethernet interfaces of the same medium (both copper or both fiber optic), or bind a copper interface to a fiber optic interface.

To set up a virtual wire, decide which two interfaces to bind (**Network > Interfaces > Ethernet**) and configure their settings as described in the following table.



If you are using an existing interface for the virtual wire, you must first remove the interface from any associated security zone.

Virtual Wire Interface Setting	Configured In	Description
Interface Name	Ethernet Interface	The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select Virtual Wire .
Virtual Wire	Ethernet Interface > Config	Select a virtual wire, or click Virtual Wire to define new Network > Virtual Wires . Select None to remove the current virtual wire assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system for the interface or click Virtual System to define a new vsys.
Security Zone		Select a security zone for the interface, or click Zone to define a new zone. Select None to remove the current zone assignment from the interface.
Link Speed	Ethernet Interface > Advanced	Select a specific interface speed in Mbps or select auto to have the firewall automatically determine the speed. Both interfaces in the virtual wire must have the same speed.
Link Duplex		Select whether the interface transmission mode is full-duplex (full), half-duplex (half), or negotiated automatically (auto). Both interfaces in the virtual wire must have the same transmission mode.
Link State		Select whether the interface status is enabled (up), disabled (down), or determined automatically (auto).

Virtual Wire Interface Setting	Configured In	Description
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		If LLDP is enabled, select an LLDP profile to assign to the interface or click LLDP Profile to create a new profile (see Network > Network Profiles > LLDP Profile). Select None to configure the firewall to use global defaults.
Enable in HA Passive State		If LLDP is enabled, select this option to configure an HA passive firewall to pre-negotiate LLDP with its peer before the firewall becomes active. If LLDP is not enabled, select this option to configure an HA passive firewall to simply pass LLDP packets through the firewall.

Virtual Wire Subinterface

▲ [Network > Interfaces > Ethernet](#)

Virtual wire (vwire) subinterfaces allow you to separate traffic by VLAN tags or a VLAN tag and IP classifier combination, assign the tagged traffic to a different zone and virtual system, and then enforce security policies for the traffic that matches the defined criteria.

To add a **Virtual Wire Interface** select the row for that interface, click **Add Subinterface**, and specify the following information.

Virtual Wire Subinterface Setting	Description
Interface Name	The read-only Interface Name displays the name of the vwire interface you selected. In the adjacent field, enter a numeric suffix (1-9999) to identify the subinterface.
Comment	Enter an optional description for the subinterface.
Tag	Enter the VLAN tag (0-4,094) for the subinterface.
Netflow Profile	If you want to export unidirectional IP traffic that traverses an ingress subinterface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Selecting None removes the current NetFlow server assignment from the subinterface.  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 Virtual Wire to define a new one (see Network > Virtual Wires). Select None to remove the current virtual wire assignment from the subinterface.
Virtual System	If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the subinterface or click Virtual System to define a new vsys.

Virtual Wire Subinterface Setting	Description
Security Zone	Select a security zone for the subinterface, or click Zone to define a new zone. Select None to remove the current zone assignment from the subinterface.

Tap Interface

▲ Network > Interfaces > Ethernet

You can use a tap interface to monitor traffic on a port.

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

Tap Interface Setting	Configured In	Description
Interface Name	Ethernet Interface	The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select Tap .
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Select None to remove the current NetFlow server assignment from the interface.  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 Virtual System to define a new vsys.
Security Zone		Select a security zone for the interface or click Zone to define a new zone. Select None to remove the current zone assignment from the interface.
Link Speed	Ethernet Interface > Advanced	Select the interface speed in Mbps (10 , 100 , or 1000), or select auto to have the firewall automatically determine the speed.
Link Duplex		Select whether the interface transmission mode is full-duplex (full), half-duplex (half), or negotiated automatically (auto).
Link State		Select whether the interface status is enabled (up), disabled (down), or determined automatically (auto).

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 with the **Log Card** type, 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.

Log Card Interface Setting	Configured In	Description
Slot	Ethernet Interface	Select the slot number (1-12) of the interface.
Interface Name		The interface name is predefined and you cannot change it.
Comment		Enter an optional description for the interface.
Interface Type		Select Log Card .
IPv4	Ethernet Interface > Log Card Forwarding	If your network uses IPv4, define the following: <ul style="list-style-type: none"> IP address—The IPv4 address of the port. Netmask—The network mask for the IPv4 address of the port. Default Gateway—The IPv4 address of the default gateway for the port.
IPv6		If your network uses IPv6, define the following: <ul style="list-style-type: none"> IP address—The IPv6 address of the port. Default Gateway—The IPv6 address of the default gateway for the port.
Link Speed	Ethernet Interface > Advanced	Select the interface speed in Mbps (10 , 100 , or 1000) or select auto (default) to have the firewall automatically determine the speed based on the connection. For interfaces that have a non-configurable speed, auto is the only option.  The minimum recommended speed for the connection is 1000 (Mbps).
Link Duplex		Select whether the interface transmission mode is full-duplex (full), half-duplex (half), or negotiated automatically based on the connection (auto). The default is auto .
Link State		Select whether the interface status is enabled (up), disabled (down), or determined automatically based on the connection (auto). The default is auto .

Log Card Subinterface

▲ Network > Interfaces > Ethernet

To add a [Log Card Interface](#), select the row for that interface, **Add Subinterface**, and specify the following information.

Log Card Subinterface Setting	Configured In	Description
Interface Name	LPC Subinterface	Interface Name (read-only) displays the name of the log card interface you selected. In the adjacent field, enter a numeric suffix (1-9,999) to identify the subinterface.
Comment		Enter an optional description for the interface.
Tag		Enter the VLAN Tag (0-4,094) for the subinterface. 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 Virtual Systems to add a new vsys. Once an LPC subinterface is assigned to a vsys, that interface is used as the source interface for all services that forward logs (syslog, email, SNMP) from the log card.
IPv4	Ethernet Interface > Log Card Forwarding	If your network uses IPv4, define the following: <ul style="list-style-type: none"> IP address—The IPv4 address of the port. Netmask—The network mask for the IPv4 address of the port. Default Gateway—The IPv4 address of the default gateway for the port.
IPv6		If your network uses IPv6, define the following: <ul style="list-style-type: none"> IP address—The IPv6 address of the port. Default Gateway—The IPv6 address of the default gateway for the port.

Decrypt Mirror Interface

▲ Network > Interfaces > Ethernet

To use the Decryption Port Mirror feature, you must select the **Decrypt Mirror** interface type. This feature enables creating a copy of decrypted traffic from a firewall and sending it to a traffic collection tool that can receive raw packet captures—such as NetWitness or Solera—for archiving and analysis. Organizations that require comprehensive data capture for forensic and historical purposes or data leak prevention (DLP) functionality require this feature. 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.

Decrypt Mirror Interface Setting	Description
Interface Name	The interface name is predefined and you cannot change it.
Comment	Enter an optional description for the interface.
Interface Type	Select Decrypt Mirror .
Link Speed	Select the interface speed in Mbps (10 , 100 , or 1000), or select auto to have the firewall automatically determine the speed.
Link Duplex	Select whether the interface transmission mode is full-duplex (full), half-duplex (half), or negotiated automatically (auto).
Link State	Select whether the interface status is enabled (up), disabled (down), or determined automatically (auto).

Aggregate Ethernet (AE) Interface Group

▲ Network > Interfaces > Ethernet

An AE interface group uses IEEE 802.1AX link aggregation to combine multiple Ethernet interfaces into a single virtual interface that connects the firewall to another network device or another firewall. An AE interface group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy; when one interface fails, the remaining interfaces continue to support traffic.

Before configuring an AE interface group, you must configure its interfaces. All the interfaces in an aggregate group must be the same with respect to bandwidth (1Gbps or 10Gbps) and interface type (HA3, virtual wire, Layer 2, or Layer 3). You can add up to eight AE interface groups per firewall and each group can have up to eight interfaces.



- All Palo Alto Networks firewalls except the PA-200 and VM-Series platforms support AE interface groups.
- You can aggregate the HA3 (packet forwarding) interfaces in a high availability (HA) active/active configuration but only on the PA-500, PA-3000 Series, PA-4000 Series, and PA-5000 Series firewalls.

To configure an AE interface group, **Add Aggregate Group**, configure the settings in the following table, and then assign interfaces to the group (see [Aggregate Ethernet \(AE\) Interface](#)).

Aggregate Interface Group Setting	Configured In	Description
Interface Name	Aggregate Ethernet Interface	The read-only Interface Name is set to ae . In the adjacent field, enter a numeric suffix (1-8) to identify the AE interface group.
Comment		Enter an optional description for the interface.
Interface Type		Select the interface type, which controls the remaining configuration requirements and options: <ul style="list-style-type: none"> • 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 (see Enable LACP). • Virtual Wire—Optionally select a Netflow Profile, and configure the Config and Advanced tabs as described in Virtual Wire Setting. • Layer 2—Optionally select a Netflow Profile; configure the Config and Advanced tabs as described in Layer 2 Interface Setting; and optionally configure the LACP tab (see Enable LACP). • Layer 3—Optionally select a Netflow Profile; configure the Config, IPv4 or IPv6, and Advanced tabs as described in Layer 3 Interface Setting; and optionally configure the LACP tab (see Enable LACP).
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Select None to remove the current NetFlow server assignment from the AE interface group. The PA-4000 Series and PA-7000 Series firewalls don't support this feature.

Aggregate Interface Group Setting	Configured In	Description
Enable LACP	Aggregate Ethernet Interface > LACP	Select this option if you want to enable Link Aggregation Control Protocol (LACP) for the AE interface group. LACP is disabled by default. If you enable LACP, interface failure detection is automatic at the physical and data link layers regardless of whether the firewall and its LACP peer are directly connected. (Without LACP, interface failure detection is automatic only at the physical layer between directly connected peers). LACP also enables automatic failover to standby interfaces if you configure hot spares (see Max Ports).
Mode		Select the LACP mode of the firewall. Between any two LACP peers, it is recommended that one is active and the other is passive. LACP cannot function if both peers are passive. <ul style="list-style-type: none"> • 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		Select the rate at which the firewall exchanges queries and responses with peer devices: <ul style="list-style-type: none"> • Fast—Every second • Slow—Every 30 seconds (this is the default setting)
Fast Failover		Select this option 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).

Aggregate Interface Group Setting	Configured In	Description
System Priority	Aggregate Ethernet Interface > LACP (cont)	The number that determines whether the firewall or its peer overrides the other with respect to port priorities (see the Max Ports field description below). Note that the lower the number, the higher the priority (range is 1-65,535; default is 32,768).
Max Ports		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 LACP port priorities of the interfaces to determine which are in standby mode. You set the LACP port priorities when configuring individual interfaces for the group (see Aggregate Ethernet (AE) Interface).
Enable in HA Passive State		For firewalls deployed in a high availability (HA) active/passive configuration, select this option to allow the passive firewall to pre-negotiate LACP with its active peer before a failover occurs. Pre-negotiation speeds up failover because the passive firewall does not have to negotiate LACP before becoming active.
Same System MAC Address for Active-Passive HA		<p>This option applies only to firewalls deployed in a high availability (HA) active/passive configuration; firewalls in an active/active configuration require unique MAC addresses.</p> <p>HA firewall peers have the same system priority value. However, in an active/passive deployment, the system ID for each can be the same or different, depending on whether you assign the same MAC address.</p> <p> When the LACP peers (also in HA mode) are virtualized (appearing to the network as a single device), using the same system MAC address for the firewalls minimizes latency during failover. When the LACP peers are not virtualized, using the unique MAC address of each firewall minimizes failover latency.</p> <p>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.</p>
MAC Address		If you enabled Use Same System MAC Address , select a system-generated MAC address, or enter your own, for both firewalls in the active/passive high availability (HA) pair. You must verify the address is globally unique.

Aggregate Ethernet (AE) Interface

▲ Network > Interfaces > Ethernet

To configure an [Aggregate Ethernet \(AE\) Interface](#), first configure an [Aggregate Ethernet \(AE\) Interface Group](#) and click the name of the interface you will assign to that group. The interface you select must be the same type as that defined for the AE interface group (for example, Layer3); you will change the type to **Aggregate Ethernet** when you configure the interface. Specify the following information for the interface.



If you enabled Link Aggregation Control Protocol (LACP) for the AE interface group, select the same **Link Speed** and **Link Duplex** for every interface in that group as a best practice. For non-matching values, the commit operation displays a warning and PAN-OS defaults to the higher speed and full duplex.

Aggregate Ethernet Interface Setting	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. If the number of interfaces you assign to the group exceeds the number of active interfaces (the Max Ports field), the firewall uses the LACP port priorities of the interfaces to determine which are in standby mode. The lower the numeric value, the higher the priority (range is 1-65535; default is 32768).

HA Interface

▲ Network > Interfaces > Ethernet

Each high availability (HA) interface has a specific function. One HA interface is for configuration synchronization and heartbeats; the other HA interface is for state synchronization. If active/active high availability is enabled, the firewall can also 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 ([Device > Virtual Systems](#)).

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

HA Interface Setting	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).

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 [Layer 2 Interface](#)) to a VLAN interface.

VLAN Interface Setting	Configure In	Description
Interface Name	VLAN Interface	The read-only Interface Name is set to <code>vlan</code> . In the adjacent field, enter a numeric suffix (1-9,999) to identify the interface.
Comment		Enter an optional description for the interface.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Select None to remove the current NetFlow server assignment from the interface.  The PA-4000 Series and PA-7000 Series firewalls don't support this feature.
VLAN	VLAN Interface > Config	Select a VLAN or click VLAN to define a new one (see Network > VLANs). Select None to remove the current VLAN assignment from the interface.
Virtual Router		Assign a virtual router to the interface, or click Virtual Router to define a new one (see Network > Virtual Routers). Select None to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click Virtual System to define a new vsys.
Security Zone		Select a security zone for the interface, or click Zone to define a new zone. Select None to remove the current zone assignment from the interface.
Management Profile		Management Profile —Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select None to remove the current profile assignment from the interface.
MTU	VLAN Interface > Advanced > Other Info	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an ICMP fragmentation needed message to the source indicating the packet is too large.
Adjust TCP MSS		Select this option to adjust the maximum segment size (MSS) to accommodate bytes for any headers within the interface MTU byte size. The MTU byte size minus the MSS Adjustment Size equals the MSS byte size, which varies by IP protocol: <ul style="list-style-type: none">• IPv4 MSS Adjustment Size—Range is 40-300; default is 40.• IPv6 MSS Adjustment Size—Range is 60-300; default is 60. Use these settings to address the case where a tunnel through the network requires a smaller MSS. If a packet has more bytes than the MSS without fragmentation, this setting enables the adjustment. Encapsulation adds length to headers, so it helps to configure the MSS adjustment size to allow bytes for such things as an MPLS header or tunneled traffic that has a VLAN tag.

VLAN Interface Setting	Configure In	Description
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 (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 this option to enable Neighbor Discovery Protocol (NDP) Proxy for the interface. The firewall will respond to ND packets requesting MAC addresses for IPv6 addresses in this list. In the ND response, the firewall sends its own MAC address for the interface, and is basically saying, “send me the packets meant for these addresses.” (Recommended) Enable NDP Proxy if you are using Network Prefix Translation IPv6 (NPTv6). If you Enable NDP Proxy , you can filter numerous Address entries. First enter a filter and then apply it (green arrow).
Address		Add one or more IPv6 addresses, IP ranges, IPv6 subnets, or address objects for which the firewall will act as NDP Proxy. Ideally, one of these addresses is the same address as that of the source translation in NPTv6. The order of addresses does not matter. If the address is a subnetwork, the firewall will send an ND response for all addresses in the subnet, so we recommend you also add the firewall’s IPv6 neighbors and then click Negate to instruct the firewall not to respond to these IP addresses.
Negate		Select Negate for an address to prevent NDP proxy for that address. You can negate a subset of the specified IP address range or IP subnet.

For an IPv4 address

Type	VLAN Interface > IPv4	Select the method for assigning an IPv4 address type to the interface: <ul style="list-style-type: none"> • Static—You must manually specify the IP address. • DHCP Client—Enables the interface to act as a Dynamic Host Configuration Protocol (DHCP) client and receive a dynamically assigned IP address.  Firewalls that are in 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.
------	---------------------------------	---

VLAN Interface Setting	Configure In	Description
IPv4 address Type = Static		
IP	VLAN Interface > IPv4	<p>Click Add, then perform one of the following steps to specify a static IP address and network mask for the interface.</p> <ul style="list-style-type: none"> Type the entry in Classless Inter-domain Routing (CIDR) notation using the format <i>ip_address/mask</i>. IPv4 example: 192.168.2.0/24 IPv6 example: 2001:db8::/32 Select an existing address object of type IP netmask. Click Address to create an address object of type IP netmask. <p>You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses.</p> <p>To delete an IP address, select the address and click Delete.</p>
IPv4 address Type = DHCP		
Enable	VLAN Interface > IPv4	Select this option to activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server		Select this option to automatically create a default route that points to the default gateway that the DHCP server provides.
Default Route Metric		For the route between the firewall and DHCP server, optionally enter a route metric (priority level) to associate with the default route and to use for path selection (range is 1-65,535, no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info		Select this option 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 option to enable IPv6 addressing on this interface.
Interface ID		Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the Use interface ID as host portion option when adding an address, the firewall uses the interface ID as the host portion of that address.

VLAN Interface Setting	Configure In	Description
Address	VLAN Interface > IPv6 (cont)	<p>Click Add and configure the following parameters for each IPv6 address:</p> <ul style="list-style-type: none"> • Address—Enter an IPv6 address and prefix length (e.g. 2001:400:f00::1/64). You can also select an existing IPv6 address object or click Address to create an address object. • Enable address on interface—Select this option to enable the IPv6 address on the interface. • Use interface ID as host portion—Select this option to use the Interface ID as the host portion of the IPv6 address. • Anycast—Select this option to include routing through the nearest node. • Send RA—Select this option 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. • Remaining fields apply only if you enable RA: <ul style="list-style-type: none"> • Valid Lifetime—The length of time (in seconds) that the firewall considers the address as valid. The valid lifetime must equal or exceed the Preferred Lifetime. The default is 2,592,000. • Preferred Lifetime—The length of time (in seconds) that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new connections but any existing connections are valid until the Valid Lifetime expires. The default is 604,800. • On-link—Select this option if systems that have addresses within the prefix are reachable without a router. • Autonomous—Select this option if systems can independently create an IP address by combining the advertised prefix with an interface ID.
Enable Duplication Address Detection		Select this option to enable duplicate address detection (DAD), then configure the other fields in this section.
DAD Attempts		Specify the number of DAD attempts within the neighbor solicitation interval (NS Interval) before the attempt to identify neighbors fails (range is 1-10; default is 1).
Reachable Time		Specify the length of time (in seconds) that a neighbor remains reachable after a successful query and response (range is 1-36,000; default is 30).
NS Interval (neighbor solicitation interval)		Specify the number of seconds for DAD attempts before failure is indicated (range is 1-10; default is 1).

VLAN Interface Setting	Configure In	Description
Enable Router Advertisement	VLAN Interface > IPv6 (cont)	To provide stateless address auto-configuration (SLAAC) on IPv6 interfaces, select this option 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, Add an address in the IP address table (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)		Specify the minimum interval (in seconds) between RAs that the firewall will send (range is 3-1,350; default is 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)		Specify the maximum interval (in seconds) between RAs that the firewall will send (range is 4-1,800; default is 600). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit		Specify the hop limit to apply to clients for outgoing packets (range is 1-255; default is 64). Enter 0 for no hop limit.
Link MTU		Specify the link maximum transmission unit (MTU) to apply to clients. Select unspecified for no link MTU (range is 1,280-9,192; default is unspecified).
Reachable Time (ms)		Specify the reachable time (in milliseconds) the client will use to assume a neighbor is reachable after receiving a reachability confirmation message. Select unspecified for no reachable time value (range is 0-3,600,000; default is unspecified).
Retrans Time (ms)		Specify the retransmission timer that determines how long the client will wait (in milliseconds) before retransmitting neighbor solicitation messages. Select unspecified for no retransmission time (range is 0-4,294,967,295; default is unspecified).
Router Lifetime (sec)		Specify how long (in seconds) the client will use the firewall as the default gateway (range is 0-9,000; default is 1,800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
Router Preference		If the network segment has multiple IPv6 routers, the client uses this field to select a preferred router. Select whether the RA advertises the firewall router as having a High , Medium (default), or Low priority relative to other routers on the segment.
Managed Configuration		Select this option to indicate to the client that addresses are available via DHCPv6.
Other Configuration		Select this option to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check		Select this option 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.

Network > Interfaces > Loopback

The following table describes loopback interface settings.

Loopback Interface Setting	Configure In	Description
Interface Name	Loopback Interface	The read-only Interface Name is set to <code>loopback</code> . In the adjacent field, enter a numeric suffix (1-9,999) to identify the interface.
Comment		Enter an optional description for the interface.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Select None to remove the current NetFlow server assignment from the interface.  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 Virtual Router to define a new one (see Network > Virtual Routers). Select None to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click Virtual System to define a new vsys.
Security Zone		Select a security zone for the interface, or click Zone to define a new zone. Select None to remove the current zone assignment from the interface.
Management Profile	Tunnel Interface > Advanced > Other Info	Management Profile —Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select None to remove the current profile assignment from the interface.
MTU		Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an ICMP fragmentation needed message to the source indicating the packet is too large.
Adjust TCP MSS		Select this option to adjust the maximum segment size (MSS) to accommodate bytes for any headers within the interface MTU byte size. The MTU byte size minus the MSS Adjustment Size equals the MSS byte size, which varies by IP protocol: <ul style="list-style-type: none">• IPv4 MSS Adjustment Size—Range is 40-300; default is 40.• IPv6 MSS Adjustment Size—Range is 60-300; default is 60. Use these settings to address the case where a tunnel through the network requires a smaller MSS. If a packet has more bytes than the MSS without fragmentation, this setting enables the adjustment. Encapsulation adds length to headers, so it helps to configure the MSS adjustment size to allow bytes for such things as an MPLS header or tunneled traffic that has a VLAN tag.

Loopback Interface Setting	Configure In	Description
For an IPv4 address		
IP	Loopback Interface > IPv4	<p>Click Add, then perform one of the following steps to specify a static IP address and network mask for the interface.</p> <ul style="list-style-type: none"> Type the entry in Classless Inter-domain Routing (CIDR) notation using the format <i>ip_address/mask</i>. IPv4 example: 192.168.2.0/24 IPv6 example: 2001:db8::/32 Select an existing address object of type IP netmask. Click Address to create an address object of type IP netmask. <p>You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses.</p> <p>To delete an IP address, select the address and click Delete.</p>
For an IPv6 address		
Enable IPv6 on the interface	Loopback Interface > IPv6	Select this option to enable IPv6 addressing on this interface.
Interface ID		Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the Use interface ID as host portion option when adding an address, the firewall uses the interface ID as the host portion of that address.
Address		<p>Click Add and configure the following parameters for each IPv6 address:</p> <ul style="list-style-type: none"> Address—Enter an IPv6 address and prefix length (for example, 2001:400:f00::1/64). You can also select an existing IPv6 address object or click Address to create an address object. Enable address on interface—Select this option to enable the IPv6 address on the interface. Use interface ID as host portion—Select this option to use the Interface ID as the host portion of the IPv6 address. Anycast—Select this option to include routing through the nearest node.

Network > Interfaces > Tunnel

The following table describes tunnel interface settings.

Tunnel Interface Setting	Configure In	Description
Interface Name	Tunnel Interface	The read-only Interface Name is set to <code>tunnel</code> . In the adjacent field, enter a numeric suffix (1-9,999) to identify the interface.
Comment		Enter an optional description for the interface.
Netflow Profile		If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click Netflow Profile to define a new profile (see Device > Server Profiles > NetFlow). Select None to remove the current NetFlow server assignment from the interface.  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 Virtual Router to define a new one (see Network > Virtual Routers). Select None to remove the current virtual router assignment from the interface.
Virtual System		If the firewall supports multiple virtual systems and that capability is enabled, select a virtual system (vsys) for the interface or click Virtual System to define a new vsys.
Security Zone		Select a security zone for the interface, or click Zone to define a new zone. Select None to remove the current zone assignment from the interface.
Management Profile	Tunnel Interface > Advanced > Other Info	Management Profile —Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Select None to remove the current profile assignment from the interface.
MTU		Enter the maximum transmission unit (MTU)  in bytes for packets sent on this interface (576-9,192; default is 1,500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an ICMP fragmentation needed message to the source indicating the packet is too large.
For an IPv4 address		
IP	Tunnel Interface > IPv4	<p>Click Add, then perform one of the following steps to specify a static IP address and network mask for the interface.</p> <ul style="list-style-type: none"> Type the entry in Classless Inter-domain Routing (CIDR) notation using the format <code>ip_address/mask</code>. IPv4 example: 192.168.2.0/24 IPv6 example: 2001:db8::/32 Select an existing address object of type IP netmask. Click Address to create an address object of type IP netmask. <p>You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses.</p> <p>To delete an IP address, select the address and click Delete.</p>

Tunnel Interface Setting	Configure In	Description
For an IPv6 address		
Enable IPv6 on the interface	Tunnel Interface > IPv6	Select this option to enable IPv6 addressing on this interface.
Interface ID	Tunnel Interface > IPv6	Enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the Use interface ID as host portion option when adding an address, the firewall uses the interface ID as the host portion of that address.
Address		<p>Click Add and configure the following parameters for each IPv6 address:</p> <ul style="list-style-type: none"> • Address—Enter an IPv6 address and prefix length (for example, 2001:400:f00::1/64). You can also select an existing IPv6 address object or click Address to create an address object. • Enable address on interface—Select this option to enable the IPv6 address on the interface. • Use interface ID as host portion—Select this option to use the Interface ID as the host portion of the IPv6 address. • Anycast—Select this option to include routing through the nearest node.

Network > Virtual Routers

The firewall requires a virtual router to obtain routes to other subnets either using static routes that you manually define, or through participation in Layer 3 routing protocols (dynamic routes). Each Layer 3 interface, loopback interface, and VLAN interface defined on the firewall must be associated with a virtual router. Each interface can belong to only one virtual router.

Defining a virtual router  requires general settings and any combination of static routes or dynamic routing protocols, as required by your network. You can also configure other features such as route redistribution and ECMP.

What do you want to know?	See:
What are the required elements of a virtual router?	General Settings of a Virtual Router
Configure:	Static Routes
	Route Redistribution
	RIP
	OSPF
	OSPFv3
	BGP
	IP Multicast
View information about a virtual router.	ECMP
	More Runtime Stats for a Virtual Router
Looking for more?	Networking 

General Settings of a Virtual Router

▲ Network > Virtual Routers > Router Settings > General

All virtual routers require that you assign Layer 3 interfaces and administrative distance metrics as described in the following table.

Virtual Router General Settings	Description
Name	Specify a name to describe the virtual router (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Interfaces	Select the interfaces that you want to include in the virtual router. Thus, they can be used as outgoing interfaces in the virtual router's routing table. To specify the interface type, refer to Network > Interfaces . When you add an interface, its connected routes are added automatically.
Administrative Distances	Specify the following administrative distances: <ul style="list-style-type: none"> Static routes—Range is 10-240; default is 10. OSPF Int—Range is 10-240; default is 30. OSPF Ext—Range is 10-240; default is 110. IBGP—Range is 10-240; default is 200. EBGP—Range is 10-240; default is 20. RIP—Range is 10-240; default is 120.

Static Routes

▲ Network > Virtual Routers > Static Routes

Optionally add one or more static routes. Click the **IP** or **IPv6** tab to specify the route using an IPv4 or IPv6 address. It is usually necessary to [configure default routes](#) (0.0.0.0/0) here. Default routes are applied for destinations that are otherwise not found in the virtual router's routing table.

Static Route Setting	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 using the format ip_address/mask: <ul style="list-style-type: none"> IPv4 example: 192.168.2.0/24 IPv6 example: 2001:db8::/32
Interface	Select the interface to forward packets to the destination, or configure the next hop settings, or both.

Static Route Setting	Description
Next Hop	Select one of the following: <ul style="list-style-type: none"> • IP Address—Select to enter the IP address of the next hop router. • Next VR—Select to 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. • Discard—Select if you want to drop traffic that is addressed to this destination. • None—Select if there is no next hop for the route.
Admin Distance	Specify the administrative distance for the static route (10-240; default is 10).
Metric	Specify a valid metric for the static route (1 - 65,535).
No Install	Select if you do not want to install the route in the route table (RIB). The route is retained in the configuration for future reference.
BFD Profile	To enable Bidirectional Forwarding Detection (BFD) for a static route on a PA-3000 Series, PA-5000 Series, PA-7000 Series, or VM-Series firewall, select one of the following: <ul style="list-style-type: none"> • default (default BFD settings) • a BFD profile that you have created on the firewall • New BFD Profile to create a new BFD profile Select None (Disable BFD) to disable BFD for the static route. To use BFD on a static route: <ul style="list-style-type: none"> • Both the firewall and the peer at the opposite end of the static route must support BFD sessions. • The static route Next Hop type must be IP Address and you must enter a valid IP address. • The Interface setting cannot be None; you must select an interface (even if you are using a DHCP address).

Route Redistribution

▲ Network > Virtual Router > Redistribution Profiles

Redistribution profiles direct the firewall to filter, set priority, and perform actions based on desired network behavior. Route redistribution allows static routes and routes that are acquired by other protocols to be advertised through specified routing protocols.

Redistribution profiles must be applied to routing protocols in order to take effect. Without redistribution rules, each protocol runs separately and does not communicate outside its purview. Redistribution profiles can be added or modified after all routing protocols are configured and the resulting network topology is established.

Apply redistribution profiles to the RIP and OSPF protocols by defining export rules. Apply redistribution profiles to BGP in the **Redistribution Rules** tab. Refer to the following table.

Redistribution Profile Setting	Description
Name	Click Add to display the Redistribution Profile page, and enter the profile name.
Priority	Enter a priority (range is 1-255) for this profile. Profiles are matched in order (lowest number first).
Redistribute	Choose whether to perform route redistribution based on the settings in this window. <ul style="list-style-type: none"> • Redist—Select to redistribute matching candidate routes. If you select this option, enter a new metric value. A lower metric value means a more preferred route. • No Redist—Select to not redistribute matching candidate routes.
General Filter Tab	
Type	Select the route types of the candidate route.
Interface	Select the interfaces to specify the forwarding interfaces of the candidate route.
Destination	To specify the destination of the candidate route, enter the destination IP address or subnet (format x.x.x.x or x.x.x.x/n) and click Add . To remove an entry, click remove ().
Next Hop	To specify the gateway of the candidate route, enter the IP address or subnet (format x.x.x.x or x.x.x.x/n) that represents the next hop and click Add . To remove an entry, click remove ().
OSPF Filter Tab	
Path Type	Select the route types of the candidate OSPF route.
Area	Specify the area identifier for the candidate OSPF route. Enter the OSPF area ID (format x.x.x.x), and click Add . To remove an entry, click remove ().
Tag	Specify OSPF tag values. Enter a numeric tag value (1-255), and click Add . To remove an entry, click remove ().

Redistribution Profile Setting	Description
BGP Filter Tab	
Community	Specify a community for BGP routing policy.
Extended Community	Specify an extended community for BGP routing policy.

RIP

▲ Network > Virtual Routers > RIP

Configuring the Routing Information Protocol (RIP) includes the following general settings.

RIP Setting	Description
Enable	Select this option to enable RIP.
Reject Default Route	(Recommended) Select this option if you do not want to learn any default routes through RIP.
BFD	To enable Bidirectional Forwarding Detection (BFD) for RIP globally for the virtual router on a PA-3000 Series, PA-5000 Series, PA-7000 Series, and VM-Series firewall, select one of the following: <ul style="list-style-type: none"> • default (profile with the default BFD settings) • a BFD profile that you have created on the firewall • New BFD Profile to create a new BFD profile Select None (Disable BFD) to disable BFD for all RIP interfaces on the virtual router; you cannot enable BFD for a single RIP interface.

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

- **Interfaces**—See [RIP Interfaces Tab](#).
- **Timers**—See [RIP Timers Tab](#).
- **Auth Profiles**—See [RIP Auth Profiles Tab](#).
- **Export Rules**—See [RIP Export Rules Tab](#).

RIP Interfaces Tab

▲ Network > Virtual Routers > RIP > Interfaces

The following table describes RIP interface settings.

RIP – Interface Setting	Description
Interface	Select the interface that runs the RIP protocol.
Enable	Select to enable these settings.
Advertise	Select to enable advertisement of a default route to RIP peers with the specified metric value.
Metric	Specify a metric value for the router advertisement. This field is visible only if you enable Advertise .
Auth Profile	Select the profile.
Mode	Select normal , passive , or send-only .
BFD	To enable BFD for a RIP interface (and thereby override the BFD setting for RIP, as long as BFD is not disabled for RIP at the virtual router level), select one of the following: <ul style="list-style-type: none"> • default (profile with the default BFD settings) • a BFD profile that you created on the firewall • New BFD Profile to create a new BFD profile Select None (Disable BFD) to disable BFD for the RIP interface.

RIP Timers Tab

▲ Network > Virtual Router > RIP > Timers

The following table describes the timers that control RIP route updates and expirations.

RIP – Timer Setting	Description
RIP Timing	
Interval Seconds (sec)	Define the length of the timer interval in seconds. This duration is used for the remaining RIP timing fields (range is 1-60).
Update Intervals	Enter the number of intervals between route update announcements (range is 1-3,600).
Expire Intervals	Enter the number of intervals between the time that the route was last updated to its expiration (range is 1-3,600).
Delete Intervals	Enter the number of intervals between the time that the route expires to its deletion (range is 1-3,600).

RIP Auth Profiles Tab

▲ Network > Virtual Router > RIP > Auth Profiles

By default, the firewall does not authenticate RIP messages between neighbors. To authenticate RIP messages between neighbors, create an authentication profile and apply it to an interface running RIP on a virtual router. The following table describes the settings for the **Auth Profiles** tab.

RIP – Auth Profile Setting	Description
Profile Name	Enter a name for the authentication profile to authenticate RIP messages.
Password Type	Select the type of password (simple or MD5). <ul style="list-style-type: none"> 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 messages, select the Preferred option.

RIP Export Rules Tab

▲ Network > Virtual Router > RIP > Export Rules

RIP export rules allow you to control which routes the virtual router sends to peers.

RIP – Export Rules Setting	Description
Allow Redistribute Default Route	Select this option to permit the firewall to redistribute its default route to peers.
Redistribution Profile	Click Add and select or create a redistribution profile that allows you to modify route redistribution, filter, priority, and action based on the desired network behavior. Refer to Route Redistribution .

OSPF

▲ Network > Virtual Router > OSPF

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

OSPF Setting	Description
Enable	Select this option to enable the OSPF protocol.
Reject Default Route	(Recommended) Select this option if you do not want to learn any default routes through OSPF.
Router ID	Specify the router ID associated with the OSPF instance in this virtual router. The OSPF protocol uses the router ID to uniquely identify the OSPF instance.
BFD	To enable Bidirectional Forwarding Detection (BFD) for OSPF globally for the virtual router on a PA-3000 Series, PA-5000 Series, PA-7000 Series, or VM-Series firewall, select one of the following: <ul style="list-style-type: none">• default (default BFD settings)• a BFD profile that you have created on the firewall• New BFD Profile to create a new BFD profile Select None (Disable BFD) to disable BFD for all OSPF interfaces on the virtual router; you cannot enable BFD for a single OSPF interface.

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

- **Areas**—See [OSPF Areas Tab](#).
- **Auth Profiles**—See [OSPF Auth Profiles Tab](#).
- **Export Rules**—See [OSPF Export Rules Tab](#).
- **Advanced**—See [OSPF Advanced Tab](#).

OSPF Areas Tab

▲ Network > Virtual Router > OSPF > Areas

The following table describes OSPF area settings.

OSPF – Areas Setting	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. <ul style="list-style-type: none"> • 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.

OSPF – Areas Setting	Description
Interface	<p>Click Add and enter the following information for each interface to be included in the area, and click OK.</p> <ul style="list-style-type: none"> • Interface—Choose the interface. • Enable—Cause the OSPF interface settings to take effect. • Passive—Select this option if you do not want the OSPF interface to send or receive OSPF packets. Although OSPF packets are not sent or received if you choose this option, the interface is included in the LSA database. • Link type—Choose Broadcast if you want all neighbors that are accessible through the interface to be discovered automatically by multicasting OSPF hello messages, such as an Ethernet interface. Choose p2p (point-to-point) to automatically discover the neighbor. Choose p2mp (point-to-multipoint) when neighbors must be defined manually. Defining neighbors manually is allowed only for p2mp mode. • Metric—Enter the OSPF metric for this interface (0-65,535). • Priority—Enter the OSPF priority for this interface (0-255). It is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) according to the OSPF protocol. When the value is zero, the router will not be elected as a DR or BDR. • Auth Profile—Select a previously-defined authentication profile. • BFD—To enable Bidirectional Forwarding Detection (BFD) for an OSPF peer interface (and thereby override the BFD setting for OSPF, as long as BFD is not disabled for OSPF at the virtual router level), select one of the following: <ul style="list-style-type: none"> • default (default BFD settings) • a BFD profile that you have created on the firewall • New BFD Profile to create a new BFD profile <p>Select None (Disable BFD) to disable BFD for the OSPF peer interface.</p> <ul style="list-style-type: none"> • Hello Interval (sec)—Interval, in seconds, at which the OSPF process sends hello packets to its directly connected neighbors (range is 0-3,600; default is 10). • Dead Counts—Number of times the hello interval can occur for a neighbor without OSPF receiving a hello packet from the neighbor, before OSPF considers that neighbor down. The Hello Interval multiplied by the Dead Counts equals the value of the dead timer (range is 3-20; default is 4). • Retransmit Interval (sec)—Length of time, in seconds, that OSPF waits to receive a link-state advertisement (LSA) from a neighbor before OSPF retransmits the LSA (range is 0-3,600; default is 10). • Transit Delay (sec)—Length of time, in seconds, that an LSA is delayed before it is sent out of an interface (range is 0-3,600; default is 1).

OSPF – Areas Setting	Description
Interface (continued)	<ul style="list-style-type: none"> • Graceful Restart Hello Delay (sec)—Applies to an OSPF interface when Active/Passive High Availability is configured. Graceful Restart Hello Delay is the length of time during which the firewall sends Grace LSA packets at 1-second intervals. During this time, no hello packets are sent from the restarting firewall. During the restart, the dead timer (which is the Hello Interval multiplied by the Dead Counts) is also counting down. If the dead timer is too short, the adjacency will go down during the graceful restart because of the hello delay. Therefore, it is recommended that the dead timer be at least four times the value of the Graceful Restart Hello Delay. For example, a Hello Interval of 10 seconds and a Dead Counts of 4 yield a dead timer of 40 seconds. If the Graceful Restart Hello Delay is set to 10 seconds, that 10-second delay of hello packets is comfortably within the 40-second dead timer, so the adjacency will not time out during a graceful restart (range is 1-10; default is 10).
Virtual Link	<p>Configure the virtual link settings to maintain or enhance backbone area connectivity. The settings must be defined for area border 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.</p> <ul style="list-style-type: none"> • Name—Enter a name for the virtual link. • Neighbor ID—Enter the router ID of the router (neighbor) on the other side of the virtual link. • Transit Area—Enter the area ID of the transit area that physically contains the virtual link. • Enable—Select to enable the virtual link. • Timing—It is recommended that you keep the default timing settings. • Auth Profile—Select a previously-defined authentication profile.

OSPF Auth Profiles Tab

▲ Network > Virtual Router > OSPF > Auth Profiles

The following table describes the OSPF Auth Profile settings.

OSPF – Auth Profile Setting	Description
Profile Name	Enter a name for the authentication profile. To authenticate the OSPF messages, first define the authentication profiles and then apply them to interfaces on the OSPF tab.
Password Type	Select the type of password (simple or MD5). <ul style="list-style-type: none"> • If you select Simple, enter the password. • If you select MD5, enter one or more password entries, including Key-ID (0-255), Key, and optional Preferred status. Click Add for each entry, and then click OK. To specify the key to be used to authenticate outgoing message, select the Preferred option.

OSPF Export Rules Tab

▲ Network > Virtual Router > OSPF > Export Rules

The following table describes the OSPF export rule settings.

OSPF – Export Rules Setting	Description
Allow Redistribute Default Route	Select this option to permit redistribution of default routes through OSPF.
Name	Select the name of a redistribution profile. The value must be an IP subnet or valid redistribution profile name.
New Path Type	Choose the metric type to apply.
New Tag	Specify a tag for the matched route that has a 32-bit value.
Metric	(Optional) Specify the route metric to be associated with the exported route and used for path selection (range is 1-65535).

OSPF Advanced Tab

▲ Network > Virtual Router > OSPF > Advanced

The following table describes the advanced settings for OSPF.

OSPF – Advanced Setting	Description
RFC 1583 Compatibility	Select this option to ensure compatibility with RFC 1583.
Timers	<ul style="list-style-type: none"> SPF Calculation Delay (sec)—Allows you to tune the delay time between receiving new topology information and performing an SPF calculation. Lower values enable faster OSPF re-convergence. Routers peering with the firewall should be tuned in a similar manner to optimize convergence times. LSA Interval (sec)—Specifies the minimum time between transmissions of two instances of the same LSA (same router, same type, same LSA ID). This is equivalent to MinLSInterval in RFC 2328. Lower values can be used to reduce re-convergence times when topology changes occur.

OSPF – Advanced Setting	Description
Graceful Restart	<ul style="list-style-type: none"> • 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 is 5-1,800; default is 120). • Max Neighbor Restart Time—The maximum grace period, in seconds, that the firewall will accept as a help-mode router. If the peer devices offers a longer grace period in its grace LSA, the firewall will not enter helper mode (range is 5-1,800; default is 140).

OSPFv3

▲ Network > Virtual Router > OSPFv3

Configuring the Open Shortest Path First v3 (OSPFv3) protocol requires configuring the first three general settings (BFD is optional).

OSPFv3 Setting	Description
Enable	Select this option to enable the OSPF protocol.
Reject Default Route	Select this option if you do not want to learn any default routes through OSPF.
Router ID	Specify the router ID associated with the OSPF instance in this virtual router. The OSPF protocol uses the router ID to uniquely identify the OSPF instance.
BFD	To enable Bidirectional Forwarding Detection (BFD) for OSPFv3 globally for the virtual router on a PA-3000 Series, PA-5000 Series, PA-7000 Series, and VM-Series firewall, select one of the following: <ul style="list-style-type: none"> • default (default BFD settings) • a BFD profile that you have created on the firewall • New BFD Profile to create a new BFD profile • (Select None (Disable BFD) to disable BFD for all OSPFv3 interfaces on the virtual router; you cannot enable BFD for a single OSPFv3 interface.)

In addition, OSPFv3 settings on the following tabs must be configured:

- **Areas**—See [OSPFv3 Areas Tab](#).
- **Auth Profiles**—See [OSPFv3 Auth Profiles Tab](#).
- **Export Rules**—See [OSPFv3 Export Rules Tab](#).
- **Advanced**—See [OSPFv3 Advanced Tab](#).

OSPFv3 Areas Tab

▲ Network > Virtual Router > OSPFv3 > Areas

The following table describes the OSPFv3 area settings.

OSPFv3 – Areas Setting	Description
Authentication	Select the name of the Authentication profile that you want to specify for this OSPF area.
Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

OSPFv3 – Areas Setting	Description
Interface	<p>Click Add and enter the following information for each interface to be included in the area, and click OK.</p> <ul style="list-style-type: none"> • Interface—Choose the interface. • Enable—Cause the OSPF interface settings to take effect. • Instance ID—Enter an OSPFv3 instance ID number. • Passive—Select this option to if you do not want the OSPF interface to send or receive OSPF packets. Although OSPF packets are not sent or received if you choose this option, the interface is included in the LSA database. • Link type—Choose Broadcast if you want all neighbors that are accessible through the interface to be discovered automatically by multicasting OSPF hello messages, such as an Ethernet interface. Choose p2p (point-to-point) to automatically discover the neighbor. Choose p2mp (point-to-multipoint) when neighbors must be defined manually. Defining neighbors manually is allowed only for p2mp mode. • Metric—Enter the OSPF metric for this interface (0-65,535). • Priority—Enter the OSPF priority for this interface (0-255). It is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) according to the OSPF protocol. When the value is zero, the router will not be elected as a DR or BDR. • Auth Profile—Select a previously-defined authentication profile. • BFD—To enable Bidirectional Forwarding Detection (BFD) for an OSPFv3 peer interface (and thereby override the BFD setting for OSPFv3, as long as BFD is not disabled for OSPFv3 at the virtual router level), select one of the following: <ul style="list-style-type: none"> • default (default BFD settings) • a BFD profile that you have created on the firewall • New BFD Profile to create a new BFD profile Select None (Disable BFD) to disable BFD for the OSPFv3 peer interface. • Hello Interval (sec)—Interval, in seconds, at which the OSPF process sends hello packets to its directly connected neighbors (range is 0-3,600; default is 10). • Dead Counts—Number of times the hello interval can occur for a neighbor without OSPF receiving a hello packet from the neighbor, before OSPF considers that neighbor down. The Hello Interval multiplied by the Dead Counts equals the value of the dead timer (range is 3-20; default is 4). • Retransmit Interval (sec)—Length of time, in seconds, that OSPF waits to receive a link-state advertisement (LSA) from a neighbor before OSPF retransmits the LSA (range is 0-3,600; default is 10). • Transit Delay (sec)—Length of time, in seconds, that an LSA is delayed before it is sent out of an interface (range is 0-3,600; default is 1).

OSPFv3 – Areas Setting	Description
Interface (continued)	<ul style="list-style-type: none"> • Graceful Restart Hello Delay (sec)—Applies to an OSPF interface when Active/Passive High Availability is configured. Graceful Restart Hello Delay is the length of time during which the firewall sends Grace LSA packets at 1-second intervals. During this time, no hello packets are sent from the restarting firewall. During the restart, the dead timer (which is the Hello Interval multiplied by the Dead Counts) is also counting down. If the dead timer is too short, the adjacency will go down during the graceful restart because of the hello delay. Therefore, it is recommended that the dead timer be at least four times the value of the Graceful Restart Hello Delay. For example, a Hello Interval of 10 seconds and a Dead Counts of 4 yield a dead timer of 40 seconds. If the Graceful Restart Hello Delay is set to 10 seconds, that 10-second delay of hello packets is comfortably within the 40-second dead timer, so the adjacency will not time out during a graceful restart (range is 1-10; default is 10). • Neighbors—For p2pmp interfaces, enter the neighbor IP address for all neighbors that are reachable through this interface.
Virtual Links	<p>Configure the virtual link settings to maintain or enhance backbone area connectivity. The settings must be defined for area border 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.</p> <ul style="list-style-type: none"> • Name—Enter a name for the virtual link. • Instance ID—Enter an OSPFv3 instance ID number. • Neighbor ID—Enter the router ID of the router (neighbor) on the other side of the virtual link. • Transit Area—Enter the area ID of the transit area that physically contains the virtual link. • Enable—Select to enable the virtual link. • Timing—It is recommended that you keep the default timing settings. • Auth Profile—Select a previously-defined authentication profile.

OSPFv3 Auth Profiles Tab

▲ Network > Virtual Router > OSPFv3 > Auth Profiles

The following table describes the OSPFv3 Auth Profile settings.

OSPF – Auth Profile Setting	Description
Profile Name	Enter a name for the authentication profile. To authenticate the OSPF messages, first define the authentication profiles and then apply them to interfaces on the OSPF tab.
SPI	Specify the security parameter index (SPI) for packet traversal from the remote firewall to the peer.
Protocol	Specify either of the following protocols: <ul style="list-style-type: none"> • ESP—Encapsulating Security Payload protocol. • AH—Authentication Header protocol

OSPF – Auth Profile Setting	Description
Crypto Algorithm	<p>Specify one of the following:</p> <ul style="list-style-type: none"> • None—No crypto algorithm will be used. • SHA1 (default)—Secure Hash Algorithm 1. • SHA256—Secure Hash Algorithm 2. A set of four hash functions with a 256 bit digest. • SHA384—Secure Hash Algorithm 2. A set of four hash functions with a 384 bit digest. • SHA512—Secure Hash Algorithm 2. A set of four hash functions with a 512 bit digest. • MD5—The MD5 message-digest algorithm.
Key/Confirm Key	Enter and confirm an authentication key.
Encryption (ESP protocol only)	<p>Specify one of the following:</p> <ul style="list-style-type: none"> • 3des (default)—applies Triple Data Encryption Algorithm (3DES) using three cryptographic keys of 56 bits. • aes-128-cbc—applies the Advanced Encryption Standard (AES) using cryptographic keys of 128 bits. • aes-192-cbc—applies the Advanced Encryption Standard (AES) using cryptographic keys of 192 bits. • aes-256-cbc—applies the Advanced Encryption Standard (AES) using cryptographic keys of 256 bits. • null—No encryption is used.
Key/Confirm Key	Enter and confirm an encryption key.

OSPFv3 Export Rules Tab

▲ Network > Virtual Router > OSPFv3 > Export Rules

The following table describes the OSPFv3 export rule settings.

OSPF – Export Rules Setting	Description
Allow Redistribute Default Route	Select this option to permit redistribution of default routes through OSPF.
Name	Select the name of a redistribution profile. The value must be an IP subnet or valid redistribution profile name.
New Path Type	Choose the metric type to apply.
New Tag	Specify a tag for the matched route that has a 32-bit value.
Metric	(Optional) Specify the route metric to be associated with the exported route and used for path selection (range is 1-65,535).

OSPFv3 Advanced Tab

▲ Network > Virtual Router > OSPFv3 > Advanced

The following table describes the advanced settings for OSPFv3.

OSPFv3 – Advanced Setting	Description
Disable Transit Routing for SPF Calculation	Select this option if you want to set the R-bit in router LSAs sent from this firewall to indicate that the firewall is not active. When in this state, the firewall participates in OSPFv3 but other routers do not send transit traffic. In this state, local traffic will still be forwarded to the firewall. This is useful while performing maintenance with a dual-homed network because traffic can be re-routed around the firewall while it can still be reached.
Timers	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 is 5-1,800; default is 120). Max Neighbor Restart Time—The maximum grace period, in seconds, that the firewall will accept as a help-mode router. If the peer devices offers a longer grace period in its grace LSA, the firewall will not enter helper mode (range is 5-800; default is 140).

BGP

▲ Network > Virtual Router > BGP

Configuring Border Gateway Protocol (BGP) requires configuring the first three settings (BFD is optional).

BGP Setting	Description
Enable	Select this option to enable BGP.
Router ID	Enter the IP address to assign to the virtual router.
AS Number	Enter the number of the AS to which the virtual router belongs, based on the router ID (range is 1-4,294,967,295).
BFD	<p>To enable Bidirectional Forwarding Detection (BFD) for BGP globally for the virtual router on a PA-3000 Series, PA-5000 Series, PA-7000 Series, or VM-Series firewall, select one of the following:</p> <ul style="list-style-type: none"> • default (default BFD settings) • a BFD profile that you have created on the firewall • New BFD Profile to create a new BFD profile <p>Select None (Disable BFD) to disable BFD for all BGP interfaces on the virtual router; you cannot enable BFD for a single BGP interface.</p> <p> If you enable or disable BFD globally, all interfaces running BGP will be taken down and brought back up with the BFD function. This can disrupt all BGP traffic. Therefore, enable BFD on BGP interfaces during an off-peak time when a reconvergence will not impact production traffic.</p>

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

- **General**—See [BGP General Tab](#).
- **Advanced**—See [BGP Advanced Tab](#).
- **Peer Group**—See [BGP Peer Group Tab](#).
- **Import**—See [BGP Import and Export Tabs](#).
- **Export**—See [BGP Import and Export Tabs](#).
- **Conditional Adv**—See [BGP Conditional Adv Tab](#).
- **Aggregate**—See [BGP Aggregate Tab](#).
- **Redist Rules**—See [BGP Redist Rules Tab](#).

BGP General Tab

▲ Network > Virtual Router > BGP > General

The following table describes the BGP general settings.

BGP – General Setting	Description
Reject Default Route	Select this option to ignore any default routes that are advertised by BGP peers.
Install Route	Select this option 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	<p>Click Add to include a new authentication profile and configure the following settings:</p> <ul style="list-style-type: none"> • Profile Name—Enter a name to identify the profile. • Secret/Confirm Secret—Enter and confirm a passphrase for BGP peer communications. <p>Click remove () to delete a profile.</p>

BGP Advanced Tab

▲ Network > Virtual Router > BGP > Advanced

The following table describes the advanced settings for BGP.

BGP – Advanced Setting	Description
Graceful Restart	<p>Activate the graceful restart option.</p> <ul style="list-style-type: none"> • Stale Route Time—Specify the length of time, in seconds, that a route can stay in the stale state (range is 1-3,600; default is 120). • Local Restart Time—Specify the length of time, in seconds, that the firewall takes to restart. This value is advertised to peers (range is 1-3,600; default is 120). • Max Peer Restart Time—Specify the maximum length of time, in seconds, that the firewall accepts as a grace period restart time for peer devices (range is 1-3,600; default is 120).
Reflector Cluster ID	Specify an IPv4 identifier to represent the reflector cluster.

BGP – Advanced Setting	Description
Confederation Member AS	Specify the identifier for the AS confederation to be presented as a single AS to external BGP peers.
Dampening Profiles	<p>Settings include:</p> <ul style="list-style-type: none"> • Profile Name—Enter a name to identify the profile. • Enable—Activate the profile. • Cutoff—Specify a route withdrawal threshold above which a route advertisement is suppressed (range is 0.0-1,000.0; default is 1.25). • Reuse—Specify a route withdrawal threshold below which a suppressed route is used again (range is 0.0-1,000.0; default is 5). • Max. Hold Time—Specify the maximum length of time, in seconds, that a route can be suppressed, regardless of how unstable it has been (range is 0-3,600; default is 900). • Decay Half Life Reachable—Specify the length of time, in seconds, after which a route's stability metric is halved if the route is considered reachable (range is 0-3,600; default is 300). • Decay Half Life Unreachable—Specify the length of time, in seconds, after which a route's stability metric is halved if the route is considered unreachable (range is 0-3,600; default is 300). <p>Click remove () to delete a profile.</p>

BGP Peer Group Tab

▲ Network > Virtual Router > BGP > Peer Group

The following table describes the BGP peer group settings.

BGP – Peer Group Setting	Description
Name	Enter a name to identify the peer.
Enable	Select to activate the peer.
Aggregated Confed AS Path	Select this option to include a path to the configured aggregated confederation AS.
Soft Reset with Stored Info	Select this option to perform a soft reset of the firewall after updating the peer settings.
Type	<p>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).</p> <ul style="list-style-type: none"> • IBGP—Specify Export Next Hop. • EBGP Confed—Specify Export Next Hop. • IBGP Confed—Specify Export Next Hop. • EBGP—Specify the following: <ul style="list-style-type: none"> • Import Next Hop • Export Next Hop • Remove Private AS (to force BGP to remove private AS numbers).

BGP – Peer Group Setting	Description
Import Next Hop	Choose an option for next hop import: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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.

BGP – Peer Group Setting	Description
Peer	<p>To add a new peer, click New and configure the following settings:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 is 0-1,200 seconds; default is 30 seconds). • Multi Hop—Set the time-to-live (TTL) value in the IP header (range is 1-255; default is 0). The default value of 0 means 2 for eBGP prior to PAN-OS 7.1.9, and it means 1 beginning with PAN-OS 7.1.9. The default value of 0 means 255 for iBGP. • Open Delay Time—Specify the delay time between opening the peer TCP connection and sending the first BGP open message (range is 0-240 seconds; default is 0 seconds). • Hold Time—Specify the period of time that may elapse between successive KEEPALIVE or UPDATE messages from a peer before the peer connection is closed. (range is 3-3,600 seconds; default is 90 seconds). • Idle Hold Time—Specify the time to wait in the idle state before retrying connection to the peer (range is 1-3,600 seconds; default is 15 seconds). • Peer Address—Specify the IP address and port of the peer. • Advanced Options—Configure the following settings: <ul style="list-style-type: none"> • 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). • BFD—To enable Bidirectional Forwarding Detection (BFD) for a BGP peer (and thereby override the BFD setting for BGP, as long as BFD is not disabled for BGP at the virtual router level), select the default profile (default BFD settings), an existing BFD profile, Inherit-vr-global-setting to inherit BGP's global BFD profile, or New BFD Profile to create a new BFD profile. Disable BFD disables BFD for the BGP peer. <p> If you enable or disable BFD globally, all interfaces running BGP will be taken down and brought back up with the BFD function. This can disrupt all BGP traffic. When you enable BFD on the interface, the firewall will stop the BGP connection to the peer to program BFD on the interface. The peer device will see the BGP connection drop, which can result in a reconvergence that impacts production traffic. Therefore, enable BFD on BGP interfaces during an off-peak time when a reconvergence will not impact production traffic.</p> <ul style="list-style-type: none"> • Incoming Connections/Outgoing Connections—Specify the incoming and outgoing port numbers and Allow traffic to or from these ports.

BGP Import and Export Tabs

- ▲ Network > Virtual Router > BGP > Import
- ▲ Network > Virtual Router > BGP > Export

The following table describes the BGP import and export settings.

BGP – Import and Export Setting	Description
Import Rules/Export Rules	<p>Click BGP Import Rules or Export Rules. To add a new rule, click Add and configure the following settings.</p> <ul style="list-style-type: none"> • General: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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—Specify an action (Allow or Deny) to take when the match conditions are met. Additionally, if and only when you specify Allow, configure the following: <ul style="list-style-type: none"> • Local Preference—Specify a local preference metric. • MED—Specify a MED value (0- 65,535). • Weight—Specify weight (0- 65,535). • Next Hop—Specify a next hop router. • Origin—Specify the path type of the originating route—IGP, EGP, or incomplete. • AS Path Limit—Specify an AS path limit. • AS Path—Specify an AS path—None, Remove, Prepend, or Remove and Prepend. • Community—Specify a community option—None, Remove All, Remove Regex, Append, or Overwrite. • Extended Community—Specify a community option—None, Remove All, Remove Regex, Append, or Overwrite. • Dampening—Specify the dampening parameter. <p>Click remove () 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.</p>

BGP Conditional Adv Tab

▲ Network > Virtual Router > BGP > Conditional Adv

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 to 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 firewall allow advertisement of the alternate route (the route to the other, non-preferred provider) as specified in its Advertise filter. To configure conditional advertisement, select the **Conditional Adv** tab and click **Add**. The following describes how to configure the values in the fields.

BGP – Conditional Adv Setting	Description
Policy	Specify the policy name for this conditional advertisement rule.
Enable	Select this option to enable BGP conditional advertisement.
Used By	Click Add and select the peer groups that will use this conditional advertisement policy.
Non Exist Filters	<p>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.</p> <p>Click Add to create a non-exist filter.</p> <ul style="list-style-type: none"> • 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.

BGP – Conditional Adv Setting	Description
Advertise Filters	<p>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.</p> <p>If a prefix is going to be advertised and does not match a Non Exist filter, the advertisement will occur.</p> <p>Click Add to create an advertise filter.</p> <ul style="list-style-type: none"> • 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.

BGP Aggregate Tab

▲ Network > Virtual Router > BGP > Aggregate

The following table describes the BGP aggregate settings.

BGP – Aggregate Setting	Description
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 route 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.

BGP Redist Rules Tab

▲ Network > Virtual Router > BGP > Redist Rules

The following table describes the BGP redistribution rule settings.

BGP – Redistribution Rule Setting	Description
Allow Redistribute Default Route	Permits the firewall to redistribute its default route to BGP peers.
Name	Enter an IP subnet or select a redistribution profile.
Enable	Click to enable this redistribution rule.
Metric	Enter a metric in the range 1-65535.
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.

IP Multicast

▲ Network > Virtual Router > Multicast

Configuring Multicast protocols requires configuring the following standard setting.

Multicast Setting	Description
Enable	Select this option to enable multicast routing.

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

- **Rendezvous Point**—See [Multicast Rendezvous Point Tab](#).
- **Interfaces**—See [Multicast Interfaces Tab](#).
- **SPT Threshold**—See [Multicast SPT Threshold Tab](#).
- **Source Specific Address Space**—See [Multicast Source Specific Address Tab](#).
- **Advanced**—See [Multicast Advanced Tab](#).

Multicast Rendezvous Point Tab

▲ Network > Virtual Router > Multicast > Rendezvous Point

The following table describes the multicast rendezvous point settings.

Multicast Setting – Rendezvous Points	Description
RP Type	<p>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.</p> <ul style="list-style-type: none"> • None—Choose if there is no RP running on this virtual router. • Static—Specify a static IP address for the RP and choose options for RP Interface and RP Address from the drop-down. Select Override learned RP for the same group if you want to use the specified RP instead of the RP elected for this group. • Candidate—Specify the following information for the candidate RP running on this virtual router: <ul style="list-style-type: none"> • 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	<p>Click Add and specify the following:</p> <ul style="list-style-type: none"> • IP address—Specify the IP address for the RP. • Override learned RP for the same group—Select this option to use the specified RP instead of the RP elected for this group. • Group—Specify a list of groups for which the specified address will act as the RP.

Multicast Interfaces Tab

▲ Network > Virtual Router > Multicast > Interfaces

The following table describes the multicast interface settings.

Multicast Setting – Interfaces	Description
Name	Enter a name to identify an interface group.
Description	Enter an optional description.
Interface	Click Add to specify one or more firewall interfaces.

Multicast Setting – Interfaces	Description
Group Permissions	<p>Specify general rules for multicast traffic:</p> <ul style="list-style-type: none"> • 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.
IGMP	<p>Specify rules for IGMP traffic. IGMP must be enabled for host facing interfaces (IGMP router) or for IGMP proxy host interfaces:</p> <ul style="list-style-type: none"> • Enable—Select this option to enable the IGMP configuration. • IGMP Version—Choose version 1, 2, or 3 to run on the interface. • Enforce Router-Alert IP Option—Select this option 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 is 1-7; default is 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: <ul style="list-style-type: none"> • 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 this option to leave the group immediately when a leave message is received.
PIM configuration	<p>Specify the following Protocol Independent Multicast (PIM) settings:</p> <ul style="list-style-type: none"> • Enable—Select this option 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 this option to use the interface as the bootstrap border. • PIM Neighbors—Click Add to specify the list of neighbors that will communicate with using PIM.

Multicast SPT Threshold Tab

▲ Network > Virtual Router > Multicast > SPT Threshold

The following table describes the multicast Shortest Path Tree (SPT) threshold settings.

Multicast Setting – SPT Thresholds	Description
Name	<p>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.</p> <p>Click Add to specify the following SPT settings:</p> <ul style="list-style-type: none"> • 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

Multicast Source Specific Address Tab

▲ Network > Virtual Router > Multicast > Source Specific Address Space

The following table describes the multicast source-specific address space settings.

Multicast Setting – Source Specific Address Spaces	Description
Name	<p>Defines the multicast groups for which the firewall will provide source-specific multicast (SSM) services.</p> <p>Click Add to specify the following settings for source-specific addresses:</p> <ul style="list-style-type: none"> • Name—Enter a name to identify this group of settings. • Group—Specify groups for the SSM address space. • Included—Select this option to include the specified groups in the SSM address space.

Multicast Advanced Tab

▲ Network > Virtual Router > Multicast > Advanced

The following table describes the advanced settings for multicast.

Multicast Advanced Setting	Description
Route Age Out Time (sec)	Allows you to tune the duration, in seconds, for which a multicast route remains in the routing table on the firewall after the session ends (range is 210-7,200; default is 210).

ECMP

▲ Network > Virtual Routers > Router Settings > ECMP

The following topics describe the Equal Cost Multiple Path (ECMP) feature.

What do you want to know?	See:
What is ECMP?	ECMP Overview
What are the fields available to configure ECMP?	ECMP Settings
Looking for more?	 ECMP

ECMP Overview

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.



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 settings shown in the following table.

ECMP Settings

▲ Network > Virtual Routers > Router Settings > ECMP

The following table describes the ECMP settings.

ECMP Setting	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	(Optional) Select Symmetric Return to cause return packets to egress out the same interface on which the associated ingress packets arrived. That is, the firewall will use the ingress interface on which to send return packets, rather than use the ECMP interface, so the Symmetric Return setting overrides load balancing. This behavior occurs only for traffic flows from the server to the client.
Max Path	Select the maximum number of equal-cost paths (2, 3, or 4) to a destination network that can be copied from the RIB to the FIB. Default is 2.
Method	Choose one of the following ECMP load-balancing algorithms to use on the virtual router. ECMP load balancing is done at the session level, not at the packet level. This means that the firewall (ECMP) chooses an equal-cost path at the start of a new session, not each time a packet is received. <ul style="list-style-type: none"> 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

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 More Runtime Stats in the last column. The window displays the following tabs:

- **Routing**—See [Routing Tab](#).
- **RIP**—See [RIP Tab](#).
- **BGP**—See [BGP Tab](#).
- **Multicast**—See [Multicast Tab](#).

Routing Tab

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

Routing Runtime Stat	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	<ul style="list-style-type: none"> ● 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. ● 01—OSPF external type-1. ● 02—OSPF external type-2. ● 0i—OSPF intra-area. ● 0o—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.

RIP Runtime Stat	Description
Summary Tab	
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 Tab	
Address	IP address of an interface on the virtual router where RIP is enabled.
Auth Type	Type of authentication—simple password, MD5, or none.
Send Allowed	Check mark indicates this interface is allowed to send RIP packets.
Receive Allowed	Check mark indicates this interface is allowed to receive RIP packets.
Advertise Default Route	Check mark indicates that RIP will advertise its default route to its peers.
Default Route Metric	Metric (hop count) assigned to the default route. The lower the metric value, the higher priority it has in the route table to be selected as the preferred path.
Key Id	Authentication key used with peers.
Preferred	Preferred key for authentication.
Peer Tab	
Peer Address	IP address of a peer to the virtual router's RIP interface.
Last Update	Date and time that the last update was received from this peer.
RIP Version	RIP version the peer is running.
Invalid Packets	Count of invalid packets received from this peer. Possible causes that the firewall cannot parse the RIP packet—x bytes over a route boundary, too many routes in packet, bad subnet, illegal address, authentication failed, or not enough memory.
Invalid Routes	Count of invalid routes received from this peer. Possible causes—route is invalid, import fails, or not enough memory.

BGP Tab

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

BGP Runtime Stat	Description
Summary Tab	
Router Id	Router ID assigned to the BGP instance.
Reject Default Route	Indicates whether the Reject Default Route option is configured, which causes the VR to ignore any default routes that are advertised by BGP peers.
Redistribute Default Route	Indicates whether the Allow Redistribute Default Route option is configured.
Install Route	Indicates whether the Install Route option is configured, which causes the VR to install BGP routes in the global routing table.
Graceful Restart	Indicates whether or not Graceful Restart is enabled (support).
AS Size	Indicates whether the AS Format size selected is 2 Byte or 4 Byte.
Local AS	Number of the AS to which the VR belongs.
Local Member AS	Local Member AS number (valid only if the VR is in a confederation). The field is 0 if the VR is not in a confederation.
Cluster ID	Displays the Reflector Cluster ID configured.
Default Local Preference	Displays the Default Local Preference configured for the VR.
Always Compare MED	Indicates whether the Always Compare MED option is configured, which enables a comparison to choose between routes from neighbors in different autonomous systems.
Aggregate Regardless MED	Indicates whether the Aggregate MED option is configured, which enables route aggregation even when routes have different MED values.
Deterministic MED Processing	Indicates whether the Deterministic MED comparison option is configured, which enables a comparison to choose between routes that are advertised by IBGP peers (BGP peers in the same AS).
Current RIB Out Entries	Number of entries in the RIB Out table.
Peak RIB Out Entries	Peak number of Adj-RIB-Out routes that have been allocated at any one time.
Peer Tab	
Name	Name of the peer.
Group	Name of the peer group to which this peer belongs.
Local IP	IP address of the BGP interface on the VR.
Peer IP	IP address of the peer.
Peer AS	Autonomous system to which the peer belongs.
Password Set	Yes or no indicates whether authentication is set.
Status	Status of the peer, such as Active, Connect, Established, Idle, OpenConfirm, or OpenSent.

BGP Runtime Stat	Description
Status Duration (sec)	Duration of the peer's status.
Peer Group Tab	
Group Name	Name of a peer group.
Type	Type of peer group configured, such as EBGP or IBGP.
Aggregate Confed. AS	Yes or no indicates whether the Aggregate Confederation AS option is configured.
Soft Reset Support	Yes or no indicates whether the peer group supports soft reset. When routing policies to a BGP peer change, routing table updates might be affected. A soft reset of BGP sessions is preferred over a hard reset because a soft reset allows routing tables to be updated without clearing the BGP sessions.
Next Hop Self	Yes or no indicates whether this option is configured.
Next Hop Third Party	Yes or no indicates whether this option is configured.
Remove Private AS	Indicates whether updates will have private AS numbers removed from the AS_PATH attribute before the update is sent.
Local RIB Tab	
Prefix	Network prefix and subnet mask in the Local Routing Information Base.
Flag	* indicates the route was chosen as the best BGP route.
Next Hop	IP address of the next hop toward the Prefix.
Peer	Name of peer.
Weight	Weight attribute assigned to the Prefix. If the firewall has more than one route to the same Prefix, the route with the highest weight is installed in the IP routing table.
Local Pref.	Local preference attribute for the route, which is used to choose the exit point toward the prefix if there are multiple exit points. A higher local preference is preferred over a lower local preference.
AS Path	List of autonomous systems in the path to the Prefix network; the list is advertised in BGP updates.
Origin	Origin attribute for the Prefix; how BGP learned of the route.
MED	Multi-Exit Discriminator (MED) attribute of the route. The MED is a metric attribute for a route, which the AS advertising the route suggests to an external AS. A lower MED is preferred over a higher MED.
Flap Count	Number of flaps for the route.
RIB Out Tab	
Prefix	Network routing entry in the Routing Information Base.
Next Hop	IP address of the next hop toward the Prefix.
Peer	Peer to which the VR will advertise this route.

BGP Runtime Stat	Description
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.

Multicast Runtime Stat	Description
FIB Tab	
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.
IGMP Interface Tab	
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 Tab	
Interface	Name of an interface to which the membership belongs.
Group	IP Multicast group address.

Multicast Runtime Stat	Description
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 Tab	
Group	IP address of the group mapped to a Rendezvous Point.
RP	IP address of Rendezvous Point for the group.
Origin	Indicates where the 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 Tab	
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 Tab	
Interface	Name of interface in the VR.
Address	IP address of the neighbor.
Secondary Address	Secondary IP address of the neighbor.

Multicast Runtime Stat	Description
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.

Network > Zones

The following topics describe network security zones.

What do you want to know?	See:
What is the purpose of a security zone?	Security Zone Overview
What are the fields available to configure security zones?	Building Blocks of Security Zones
Looking for more?	Segment Your Network Using Interfaces and Zones 

Security Zone Overview

Security zones are a logical way to group physical and virtual interfaces on the firewall in order to control and log the traffic that traverses (through these interface on) your network. An interface on the firewall must be assigned to a security zone before the interface can process traffic. A zone can have multiple interfaces of the same type (for example, tap, layer 2 or layer 3 interfaces) assigned to it, but an interface can belong to only one zone.

Policy rules on the firewall use security zones to identify where the traffic comes from and where it is going. Traffic can flow freely within a zone, but traffic will not be able to flow between different zones until you define a security policy rule that allows it. For inter-zone traffic, security policy rules must reference a source zone and destination zone (not interfaces) to allow or deny traffic. The zones must be of the same type, that is, a security policy rule can allow or deny traffic from one Layer 2 zone to another Layer 2 zone only.

Building Blocks of Security Zones

To define a security zone, click **Add** and specify the following information.

Security Zone Setting	Description
Name	Enter a zone name (up to 31 characters). This name appears in the list of zones when defining security policies and configuring interfaces. The name is case-sensitive and must be unique within the virtual router. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Location	This field is present only if the firewall supports multiple virtual systems (vsys) and that capability is enabled. Select the vsys to which this zone applies.

Security Zone Setting	Description
Type	<p>Select a zone type (Tap, Virtual Wire, Layer2, Layer3, or External) to view all the Interfaces of that type that have not been assigned to a zone. The Layer 2 and Layer 3 zone types list all Ethernet interfaces and subinterfaces of that type. Add the interfaces that you want to assign to the zone.</p> <p>The External zone is used to control traffic between multiple virtual systems on a single firewall. It displays only on firewalls that support multiple virtual systems and only if the Multi Virtual System Capability is enabled. For information on external zones, see Inter-VSYS Traffic that Remains Within the Firewall.</p> <p>An interface can belong to only one zone in one virtual system.</p>
Service Profile Zone for NSX	<p>(VM-Series NSX edition firewalls only) On Panorama, select this option to create one or more zones within a template that is used to deploy the VM-Series NSX edition firewall.</p> <p>When you select this option, Panorama automatically generates a pair of subinterfaces configured in a virtual wire and then pushes the pair to the VM-Series firewalls included in the template. On a Panorama commit, this zone becomes available as a <i>service profile</i> on the NSX Manager. You can use the service profile on the NSX Manager user interface to redirect traffic to the VM-Series firewalls that are configured with this zone.</p> <p>Before you select Service Profile Zone for NSX, make sure you select the correct template in the Template drop-down. The template name must match the name you specified in the VMware Service Definitions (Panorama > VMware Service Manager).</p> <p> The virtual wire subinterfaces that are automatically created are not displayed under Network > Interfaces on the VM-Series firewall or on Panorama.</p> <p>You cannot manually select or assign the interfaces to the Service Profile Zone for NSX. Panorama creates a pair of subinterfaces that are configured in a virtual wire and assigns them to the zone.</p> <p>To enforce policy, you must use the same zone name as the source zone and the destination zone in a security policy prerule on Panorama. For more information, see Set Up the VM-Series NSX Edition Firewall.</p>
Interfaces	Add one or more interfaces to this zone.
Zone Protection Profiles	Select a profile that specifies how the security gateway responds to attacks from this zone. To create a new profile, refer to Network > Network Profiles > Zone Protection .
Log Setting	<p>Select a Log Forwarding profile for forwarding zone protection logs to an external system.</p> <p>If you have a Log Forwarding profile named <i>default</i>, that profile will be automatically selected for this drop-down when defining a new security zone. You can override this default setting at any time by continuing to select a different Log Forwarding profile when setting up a new security zone. To define or add a new Log Forwarding profile (and to name a profile <i>default</i> so that this drop-down is populated automatically), click New (refer to Objects > Log Forwarding).</p> <p> If you are configuring the zone in a Panorama template, the Log Setting drop-down lists only shared Log Forwarding profiles; to specify a non-shared profile, you must type its name.</p>

Security Zone Setting	Description
Enable User Identification	<p>If you configured User-ID™ to perform IP address-to-username mapping (discovery), select this option to apply the mapping information to traffic in this zone. If you disable this option, firewall logs, reports, and policies will exclude user mapping information for traffic within the zone.</p> <p>By default, if you select this option, the firewall applies user mapping information to the traffic of all subnetworks in the zone. To limit the information to specific subnetworks within the zone, use the Include List and Exclude List.</p> <p> User-ID performs discovery for the zone only if it falls within the network range that User-ID monitors. If the zone is outside that range, the firewall does not apply user mapping information to the zone traffic even if you select Enable User Identification. For details, see Define Subnetworks to Include/Exclude for User Mapping.</p> <p> Enable User-ID on trusted zones only. If you enable User-ID and client probing on an external untrusted zone (such as the internet), probes could be sent outside your protected network, resulting in an information disclosure of the User-ID agent service account name, domain name, and encrypted password hash, which could allow an attacker to gain unauthorized access to protected resources.</p>
User Identification ACL Include List	<p>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.</p> <p>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.</p> <p>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. For details, see Define Subnetworks to Include/Exclude for User Mapping.</p>
User Identification ACL Exclude List	<p>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.</p> <p> 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.</p>

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.

VLAN Setting	Description
Name	Enter a VLAN name (up to 31 characters). This name appears in the list of VLANs when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
VLAN Interface	Select a Network > Interfaces > VLAN to allow traffic to be routed outside the VLAN.
Interfaces	Specify firewall interfaces for the VLAN.
Static MAC Configuration	Specify the interface through which a MAC address is reachable. This will override any learned interface-to-MAC mappings.

Network > IPSec Tunnels

Select **Network > IPSec Tunnels** to establish and manage IPSec VPN tunnels between firewalls. This is the Phase 2 portion of the IKE/IPSec VPN setup.

What do you want to know?	See:
Manage IPsec VPN tunnels.	IPSec VPN Tunnel Management
Configure an IPsec tunnel.	IPSec Tunnel General Tab
	IPSec Tunnel Proxy IDs Tab
View IPsec tunnel status.	IPSec Tunnel Status on the Firewall
Restart or refresh an IPsec tunnel.	IPSec Tunnel Restart or Refresh
Looking for more?	Set up an IPSec tunnel 

IPSec VPN Tunnel Management

The following table describes how to manage your IPSec VPN tunnels.

Fields to Manage IPSec VPN Tunnels	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

The following table describes the IPSec tunnel general settings.

IPSec Tunnel General Setting	Description
Name	<p>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.</p> <p>The 63-character limit for this field includes the tunnel name in addition to the Proxy ID, which is separated by a colon character.</p>
Tunnel Interface	Select an existing tunnel interface, or click New Tunnel Interface . For information on creating a tunnel interface, refer to Network > Interfaces > Tunnel .
IPv4 or IPv6	Select IPv4 or IPv6 to configure the tunnel to have endpoints with that IP type of address.
Type	Select whether to use an automatically generated or manually entered security key. Auto key is recommended.
Auto Key	<p>If you choose Auto Key, specify the following:</p> <ul style="list-style-type: none"> • IKE Gateway—Refer to Network > Network Profiles > IKE Gateways for descriptions of the IKE gateway settings. • IPSec Crypto Profile—Select an existing profile or keep the default profile. To define a new profile, click New and follow the instructions in Network > Network Profiles > IPSec Crypto. • Click Show Advanced Options to access the remaining fields. • Enable Replay Protection—Select 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. <ul style="list-style-type: none"> • Destination IP—Specify an IP address on the other side of the tunnel that the tunnel monitor will use to determine if the tunnel is working properly. • Profile—Select an existing profile that will determine the actions that are taken if the tunnel fails. If the action specified in the monitor profile is wait-recover, the firewall will wait for the tunnel to become functional and will NOT seek an alternate path with the route table. If the fail-over action is used, the firewall will check the route table to see if there is an alternate route that can be used to reach the destination. For more information, see Network > Network Profiles > Monitor.

IPSec Tunnel General Setting	Description
Manual Key	<p>If you choose Manual Key, specify the following:</p> <ul style="list-style-type: none"> • Local SPI—Specify the local security parameter index (SPI) for packet traversal from the local firewall to the peer. SPI is a hexadecimal index that is added to the header for IPSec tunneling to assist in differentiating between IPSec traffic flows. • Interface—Select the interface that is the tunnel endpoint. • Local Address—Select the IP address for the local interface that is the endpoint of the tunnel. • Remote SPI—Specify the remote security parameter index (SPI) for packet traversal from the remote firewall to the peer. • Protocol—Choose the protocol for traffic through the tunnel (ESP or AH). • Authentication—Choose the authentication type for tunnel access (SHA1, SHA256, SHA384, SHA512, MD5, or None). • Key/Confirm Key—Enter and confirm an authentication key. • Encryption—Select an encryption option for tunnel traffic (3des, aes-128-cbc, aes-192-cbc, aes-256-cbc, des, or null [no encryption]). • Key/Confirm Key—Enter and confirm an encryption key.
GlobalProtect Satellite	<p>If you choose GlobalProtect Satellite, specify the following:</p> <ul style="list-style-type: none"> • 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 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 satellite and select the Local Certificate and the Certificate Profile.

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.

Proxy IDs IPv4 and IPv6 Setting	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:prefix-length (or per IPv6 convention, for example, 2001:DB8:0::/48). IPv6 addressing does not require that all zeros be written; leading zeros can be omitted and one grouping of consecutive zeros can be replaced by two adjacent colons (::). For an IKEv2 traffic selector, this field is converted to Source IP Address.
Remote	If required by the peer: <ul style="list-style-type: none"> • 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: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: <ul style="list-style-type: none"> • Number—Specify the protocol number (used for interoperability with third-party devices). • Any—Allow TCP and/or UDP traffic. • TCP—Specify the local and remote TCP port numbers. • UDP—Specify the local and remote UDP port numbers. Each configured proxy ID will count towards the IPSec VPN tunnel capacity of the firewall. This field is also used as an IKEv2 traffic selector.

IPSec Tunnel Status on the Firewall

To view the status of currently defined IPSec VPN tunnels, open the **IPSec Tunnels** page. The following status information is reported on the page:

- **Tunnel Status (first status column)**—Green indicates an IPSec phase-2 security association (SA) tunnel. Red indicates that IPSec phase-2 SA is not available or has expired.
- **IKE Gateway Status**—Green indicates a valid IKE phase-1 SA or IKEv2 IKE SA. Red indicates that IKE phase-1 SA is not available or has expired.
- **Tunnel Interface Status**—Green indicates that the tunnel interface is up (because tunnel monitor is disabled or because tunnel monitor status is UP and the monitoring IP address is reachable). Red indicates that the tunnel interface is down because the tunnel monitor is enabled and the remote tunnel monitoring IP address is unreachable.

IPSec Tunnel Restart or Refresh

Select **Network > IPSec Tunnels** to display status of tunnels. In the first Status column is a link to the **Tunnel Info**. Click the tunnel you want to restart or refresh to open the **Tunnel Info** page for that tunnel. Click on one of entries in the list and then click:

- **Restart**—Restart the selected tunnel. A restart disrupts traffic going across the tunnel.
- **Refresh**—Show the current IPSec SA status.

Network > 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 do you want to know?	See:
What is DHCP?	DHCP Overview
How does a DHCP server allocate addresses?	DHCP Addressing
Configure an interface on the firewall to act as a:	DHCP Server
	DHCP Relay
	Network > DNS Proxy
Looking for more?	 DHCP

DHCP Overview

▲ Network > DHCP

DHCP uses a client-server model of communication. This model consists of three roles that the firewall can fulfill:

- **DHCP client**—A firewall acting as a DHCP client (host) can request an IP address and other configuration settings from a DHCP server. Users on client firewalls save configuration time and effort, and need not know the addressing plan of the network or other network resources and options inherited from the DHCP server.
- **DHCP server**—A firewall acting as a DHCP server can service clients. By using one of the DHCP addressing mechanisms, the administrator saves configuration time and has the benefit of reusing a limited number of IP addresses clients no longer need network connectivity. The server can also deliver IP addressing and DHCP options to multiple clients.
- **DHCP relay agent**—A firewall acting as a DHCP relay agent listens for broadcast and unicast DHCP messages and relays them between DHCP clients and servers.

DHCP uses [User Datagram Protocol \(UDP\)](#), [RFC 768](#), as its transport protocol. DHCP messages that a client sends to a server are sent to well-known port 67 (UDP—Bootstrap Protocol and DHCP). DHCP messages that a server sends to a client are sent to port 68.

DHCP Addressing

There are three ways that a DHCP server either assigns or sends an IP address to a client:

- **Automatic allocation**—The DHCP server assigns a permanent IP address to a client from its **IP Pools**. On the firewall, a **Lease** specified as **Unlimited** means the allocation is permanent.
- **Dynamic allocation**—The DHCP server assigns a reusable IP address from **IP Pools** of addresses to a client for a maximum period of time, known as a *lease*. This method of address allocation is useful when the customer has a limited number of IP addresses; they can be assigned to clients who need only temporary access to the network.
- **Static allocation**—The network administrator chooses the IP address to assign to the client and the DHCP server sends it to the client. A static DHCP allocation is permanent; it is done by configuring a DHCP server and choosing a **Reserved Address** to correspond to the **MAC Address** of the client firewall. The DHCP assignment remains in place even if the client disconnects (logs off, reboots, has a power outage, etc.). Static allocation of an IP address is useful, for example, if you have a printer on a LAN and you do not want its IP address to keep changing, because it is associated with a printer name through DNS. Another example is if a client firewall is used for something crucial and must keep the same IP address, even if the firewall is turned off, unplugged, rebooted, or a power outage occurs.

Keep the following points in mind when configuring a **Reserved Address**:

- It is an address from the **IP Pools**. You can configure multiple reserved addresses.
- If you configure no **Reserved Address**, the clients of the server will receive new DHCP assignments from the pool when their leases expire or if they reboot, etc. (unless you specified that a **Lease** is **Unlimited**).
- If you allocate every address in the **IP Pools** as a **Reserved Address**, there are no dynamic addresses free to assign to the next DHCP client requesting an address.
- You may configure a **Reserved Address** without configuring a **MAC Address**. In this case, the DHCP server will not assign the **Reserved Address** to any firewall. You might reserve a few addresses from the pool and statically assign them to a fax and printer, for example, without using DHCP.

DHCP Server

▲ Network > DHCP > DHCP Server

The following section describes each component of the DHCP server. Before you configure a DHCP server, you should already have configured a Layer 3 Ethernet or Layer 3 VLAN interface that is assigned to a virtual router and a zone. You should also know a valid pool of IP addresses from your network plan that can be designated to be assigned by your DHCP server to clients.

When you add a DHCP server, you configure the settings described in the table below.

DHCP Server Settings	Configured In	Description
Interface	DHCP Server	Name of the interface that will serve as the DHCP server.
Mode		Select enabled or auto mode. Auto mode enables the server and disables it if another DHCP server is detected on the network. The disabled setting disables the server.

DHCP Server Settings	Configured In	Description
Ping IP when allocating new IP	DHCP Server > Lease	If you click Ping IP when allocating new IP , the server will ping the IP address before it assigns that address to its client. If the ping receives a response, that means a different firewall already has that address, so it is not available for assignment. The server assigns the next address from the pool instead. If you select this option, the Probe IP column in the display will have a check mark.
Lease		<p>Specify a lease type.</p> <ul style="list-style-type: none"> • 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		<p>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.</p>
Reserved Address		<p>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.</p> <p>If you also specify a MAC Address (format xx:xx:xx:xx:xx:xx), the Reserved Address is assigned to the firewall associated with that MAC address when that firewall requests an IP address through DHCP.</p>
Inheritance Source	DHCP Server > Options	<p>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.</p> <p>One benefit of specifying an inheritance source is that DHCP options are quickly transferred from the server that is upstream of the source DHCP client. It also keeps the client's options updated if an option on the inheritance source is changed. For example, if the inheritance source firewall replaces its NTP server (which had been identified as the Primary NTP server), the client will automatically inherit the new address as its Primary NTP server.</p>
Check inheritance source status		<p>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.</p>

DHCP Server Settings	Configured In	Description
Gateway	DHCP Server > Options (cont)	Specify the IP address of the network gateway (an interface on the firewall) that is used to reach any device not on the same LAN as this DHCP server.
Subnet Mask		Specify the network mask that applies to the addresses in the IP Pools .
Options		<p>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.</p> <p>The DHCP server sends these settings to its clients.</p> <ul style="list-style-type: none"> • Primary DNS, Secondary DNS—IP address of the preferred and alternate Domain Name System (DNS) servers. • Primary WINS, Secondary WINS—IP address of the preferred and alternate Windows Internet Name Service (WINS) servers. • Primary NIS, Secondary NIS—IP address of the preferred and alternate Network Information Service (NIS) servers. • Primary NTP, Secondary NTP—IP address of the available network time protocol (NTP) servers. • POP3 Server—IP address of a Post Office Protocol version 3 (POP3) server. • SMTP Server—IP address of a Simple Mail Transfer Protocol (SMTP) server. • DNS Suffix—Suffix for the client to use locally when an unqualified hostname is entered that the client cannot resolve.
Custom DHCP options		<p>Click Add and enter the Name of the custom option you want the DHCP Server to send to clients.</p> <p>Enter an Option Code (range is 1-254).</p> <p>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.</p> <p>Click Inherited from DCHP server inheritance source to have the server inherit the value for that option code from the inheritance source.</p> <p>Alternatively, for Option Type, select IP Address, ASCII, or Hexadecimal to specify the type of data used for the Option Value and, for Option Value, click Add to enter the value for the custom option.</p>

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. Each interface can forward messages to a maximum of eight external IPv4 DHCP servers and eight external IPv6 DHCP servers. A client sends a DHCPDISCOVER message to all configured servers, and the firewall relays the DHCPOFFER message of the first server that responds back to the requesting client.

DHCP Relay Setting	Description
Interface	Name of the interface that will be the DHCP relay agent.
IPv4 / IPv6	Select the type of DHCP server and IP address you will specify.
DHCP Server IP Address	Enter the IP address of the DHCP server to and from which you will relay DHCP messages.
Interface	If you selected IPv6 as the IP address protocol for the DHCP server and specified a multicast address, you must also specify an outgoing interface.

DHCP Client

- ▲ Network > Interfaces > Ethernet > IPv4
 ▲ Network > Interfaces > VLAN > IPv4

Before [configuring a firewall interface as a DHCP client](#), make sure you have configured a Layer 3 Ethernet or Layer 3 VLAN interface and that you assigned the interface to a virtual router and a zone. Perform this task if you need to use DHCP to request an IPv4 address for an interface on your firewall.

DHCP Client Setting	Description
Type	Select DHCP Client and then Enable to configure the interface as a DHCP client.
Automatically create default route pointing to default gateway provided by server	Causes the firewall to create a static route to a default gateway that will be useful when clients are trying to access many destinations that do not need to have routes maintained in a routing table on the firewall.
Default Route Metric	Optionally, enter a Default Route Metric (priority level) for the route between the firewall and the DHCP server. A route with a lower number has higher priority during route selection. For example, a route with a metric of 10 is used before a route with a metric of 100 (range is 1-65,535; no default).
Show DHCP Client Runtime Info	Displays all settings received from the DHCP server, including DHCP lease status, dynamic IP assignment, subnet mask, gateway, and server settings (DNS, NTP, domain, WINS, NIS, POP3, and SMTP).

Network > DNS Proxy

DNS servers perform the service of resolving a domain name with an IP address and vice versa. When you configure the firewall as a DNS proxy, it acts as an intermediary between clients and servers and as a DNS server by resolving queries from its DNS cache or forwarding queries to other DNS servers. Use this page to configure the settings that determine how the firewall serves as a DNS proxy.

What do you want to know?	See:
How does the firewall proxy DNS requests?	DNS Proxy Overview
How do I configure a DNS proxy?	
How do I configure static FQDN-to-IP address mappings?	DNS Proxy Settings
What actions can I perform to manage DNS proxies?	Additional DNS Proxy Actions
Want more information?	DNS

DNS Proxy Overview

You can configure the firewall to act as a DNS server by creating a DNS proxy, selecting the interfaces the proxy applies to, and specifying the default DNS primary and secondary servers to which the firewall sends the DNS queries if it doesn't find the domain name in its DNS proxy cache (and if the domain name doesn't match a proxy rule).

To direct DNS queries to different DNS servers based on domain names, you can create DNS proxy rules. Specifying multiple DNS servers can ensure localization of DNS queries and increase efficiency. For example, you can forward all corporate DNS queries to a corporate DNS server and forward all other queries to ISP DNS servers.

Use the following tabs to define a DNS proxy (beyond the default DNS primary and secondary servers):

- **Static Entries**—Allows you to configure static FQDN-to-IP address mappings that the firewall caches and sends to hosts in response to DNS queries.
- **DNS Proxy Rules**—Allows you to specify domain names and corresponding primary and secondary DNS servers to resolve queries that match the rule. If the domain name isn't in the DNS proxy cache, the firewall searches for a match in the DNS proxy (on the interface on which the query arrived), and forwards the query to a DNS server based on the match results. If no match is found, the firewall sends the query to the default DNS primary and secondary servers. You can enable caching of domains that match the rule.
- **Advanced**—Allows you to enable caching and control TCP queries and UDP Query Retries.

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.

DNS Proxy Settings

Click **Add** and configure the firewall to act as a DNS proxy. You can configure a maximum of 256 DNS proxies on a firewall.

DNS Proxy Setting	Configured In	Description
Enable	DNS Proxy	Select this option to enable DNS proxy.
Name		Specify a name to identify the DNS proxy object (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location		Specify the virtual system to which the DNS proxy object applies. 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. Select Device > Virtual Systems , select a virtual system, and select a DNS Proxy .
Inheritance Source		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		Select this option 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		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		Specify the IP addresses of the default primary and secondary DNS servers to which this firewall (as DNS proxy) sends DNS queries. If the primary DNS server cannot be found, the secondary is used.
Interface		<p>Select Interface to specify the firewall interfaces to support the DNS proxy rules. Select an interface from the drop-down and click Add. You can add multiple interfaces. To delete an interface, select the interface and click Delete.</p> <p>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).</p>

DNS Proxy Setting	Configured In	Description
Name	DNS Proxy > DNS Proxy Rules	A name is required so that an entry can be referenced and modified via the CLI.
Turn on caching of domains resolved by this mapping		Select this option to enable caching of domains that are resolved by this mapping.
Domain Name		Click Add and enter one or more domain names to which the firewall compares incoming FQDNs. If the FQDN matches one of the domains in the rule, the firewall forwards the query to the Primary/Secondary DNS server specified for this proxy. To delete a domain name from the rule, select it and click Delete .
Primary/Secondary		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.
FQDN		Enter the Fully Qualified Domain Name (FQDN) that will be mapped to the static IP addresses defined in the Address field.
Address		Click Add and enter one or more IP addresses that map to this domain. The firewall includes all of these addresses in its DNS response, and the client chooses which IP address to use. To delete an address, select the address and click Delete .
Cache	DNS Proxy > Advanced	Select this option to enable DNS caching. Leave Size and Timeout settings with default values. Beginning with PAN-OS 7.1.1 and for later releases, the DNS proxy automates these settings to maximize efficiency.
TCP Queries		Select this option to enable DNS queries using TCP. Specify the upper limit on the number of concurrent pending TCP DNS requests (Max Pending Requests) that the firewall will support (range is 64-256; default is 64).
UDP Queries Retries		Specify settings for UDP query retries: <ul style="list-style-type: none"> • Interval—Specify the time, in seconds, after which another request is sent if no response has been received (range is 1-30; default is 2). • Attempts—Specify the maximum number of attempts (excluding the first attempt) after which the next DNS server is tried (range is 1-30; default is 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 clear the **Enable** option. To enable a DNS proxy that is disabled, click into the name of the DNS proxy entry and select **Enable**.

Network > QoS

The following topics describe Quality of Service (QoS).

What do you want to know?	See:
Set bandwidth limits for an interface and enforce QoS for traffic exiting an interface.	QoS Interface Settings
Monitor traffic exiting a QoS-enabled interface.	QoS Interface Statistics
Looking for more?	<p>See Quality of Service for complete QoS workflows, concepts and use cases.</p> <p>Select Policies > QoS to assign matched traffic a QoS class, or select Network > Network Profiles > QoS to define bandwidth limits and priority for up to eight QoS classes.</p>

QoS Interface Settings

Enable QoS on an interface to set bandwidth limits for the interface and/or to enable the interface to enforce QoS for egress traffic. Enabling a QoS interface includes attaching a QoS profile to the interface. QoS is supported on physical interfaces and, depending on firewall 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.

To get started, **Add** or modify a QoS Interface, and then define the fields described in the following table.

QoS Interface Setting	Configured In	Description
Interface Name		Select the firewall interface on which to enable QoS.
Egress Max (Mbps)	QoS Interface > Physical Interface	Enter the limit on traffic leaving the firewall through this interface.  Though this is not a required field, we recommend always defining the Egress Max value for a QoS interface.
Turn on QoS feature on this interface		Select this option 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 Network > Network Profiles > QoS .
Tunnel Interface		

QoS Interface Setting	Configured In	Description
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.
Add		<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Name—Enter a name to identify these settings. • QoS Profile—Select the QoS profile to apply to the specified interface and subnet. For instructions on defining QoS profiles, refer to Network > Network Profiles > QoS. • Source Interface—Select the firewall interface. • 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: <ul style="list-style-type: none"> • Tunnel Interface—Select the tunnel interface on the firewall. • QoS Profile—Select the QoS profile to apply to the specified tunnel interface. <p>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.</p> <p>To remove a clear text or tunneled traffic entry, clear the entry and click Delete.</p> <p>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.</p>

QoS Interface Statistics

▲ Network > QoS > Statistics

For a QoS interface, select **Statistics** to view bandwidth, session, and application information for configured QoS interfaces.

QoS Statistic	Description
Bandwidth	<p>Shows the real time bandwidth charts for the selected node and classes. This information is updated every two seconds.</p>  <p>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.</p>
Applications	Lists all active applications for the selected QoS node and/or class.
Source Users	Lists all the active source users for the selected QoS node and/or class.
Destination Users	Lists all the active destination users for the selected QoS node and/or class.
Security Rules	Lists the security rules matched to and enforcing the selected QoS node and/or class.
QoS Rules	Lists the QoS rules matched to and enforcing the selected QoS node and/or class.

Network > LLDP

Link Layer Discovery Protocol (LLDP) provides an automatic method of discovering neighboring devices and their capabilities at the Link Layer.

What do you want to know?	See:
What is LLDP?	LLDP Overview
Configure LLDP.	Building Blocks of LLDP
Configure an LLDP profile.	Network > Network Profiles > LLDP Profile
Looking for more?	LLDP

LLDP Overview

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

Building Blocks of LLDP

To enable LLDP on the firewall, click Edit, click **Enable**, and optionally configure the four settings shown in the following table, if the default settings do not suit your environment. The remaining table entries describe the status and peer statistics.

LLDP Setting	Configured In	Description
Transmit Interval (sec)	LLDP General	Specify the interval, in seconds, at which LLDPDUs are transmitted (range is 1-3,600; default is 30).
Transmit Delay (sec)		Specify the delay time, in seconds, between LLDP transmissions sent after a change is made in a Type-Length-Value (TLV) element. The delay helps to prevent flooding the segment with LLDPDUs if many network changes spike the number of LLDP changes or if the interface flaps. The Transmit Delay must be less than the Transmit Interval (range is 1-600; default is 2).
Hold Time Multiple		Specify a value that is multiplied by the Transmit Interval to determine the total TTL hold time (range is 1-100; default is 4). The TTL hold time is the length of time the firewall will retain the information from the peer as valid. The maximum TTL hold time is 65,535 seconds, regardless of the multiplier value.
Notification Interval		Specify the interval, in seconds, at which syslog and SNMP Trap notifications are transmitted when MIB changes occur (range is 1-3,600; default is 5).

LLDP Setting	Configured In	Description
spyglass filter	LLDP > Status	Optionally enter a data value in the filter row and click the gray arrow, which causes only the rows that include that data value to be displayed. Click the red X to Clear Filter.
Interface		Name of the interfaces that have LLDP profiles assigned to them.
LLDP		LLDP status—enabled or disabled.
Mode		LLDP mode of the interface—Tx/Rx, Tx Only, or Rx Only.
Profile		Name of the profile assigned to the interface.
Total Transmitted		Count of LLDPDUs transmitted out the interface.
Dropped Transmit		Count of LLDPDUs that were not transmitted out the interface because of an error. For example, a length error when the system is constructing an LLDPDU for transmission.
Total Received		Count of LLDP frames received on the interface.
Dropped TLV		Count of LLDP frames discarded upon receipt.
Errors		Count of Time-Length-Value (TLV) elements that were received on the interface and contained errors. Types of TLV errors include—one or more mandatory TLVs missing, out of order, containing out-of-range information, or length error.
Unrecognized		Count of TLVs received on the interface that are not recognized by the LLDP local agent, for example, because the TLV type is in the reserved TLV range.
Aged Out		Count of items deleted from the Receive MIB due to proper TTL expiration.
Clear LLDP Statistics		Select this option to clear all of the LLDP statistics.

LLDP Setting	Configured In	Description
spyglass filter	LLDP > Peers	Optionally enter a data value in the filter row and click the gray arrow, which causes only the rows that include that data value to be displayed. Click the red X to Clear Filter.
Local Interface		Interface on the firewall that detected the neighboring device.
Remote Chassis ID		Chassis ID of the peer; the MAC address is used.
Port ID		Port ID of the peer.
Name		Name of the peer.
More Info		Click More Info to see Remote Peer Details, which are based on the Mandatory and Optional TLVs.
Chassis Type		Chassis Type is MAC address.
MAC Address		MAC address of the peer.
System Name		Name of the peer.
System Description		Description of the peer.
Port Description		Port description of the peer.
Port Type		Interface name.
Port ID		Firewall uses the ifname of the interface.
System Capabilities		Capabilities of the system. O=Other, P=Repeater, B=Bridge, W=Wireless-LAN, R=Router, T=Telephone
Enabled Capabilities		Capabilities enabled on the peer.
Management Address		Management address of the peer.

Network > Network Profiles

- ▲ [Network > Network Profiles > GlobalProtect IPSec Crypto](#)
- ▲ [Network > Network Profiles > IKE Gateways](#)
- ▲ [Network > Network Profiles > IPSec Crypto](#)
- ▲ [Network > Network Profiles > IKE Crypto](#)
- ▲ [Network > Network Profiles > Interface Mgmt](#)
- ▲ [Network > Network Profiles > Monitor](#)
- ▲ [Network > Network Profiles > Zone Protection](#)
- ▲ [Network > Network Profiles > LLDP Profile](#)
- ▲ [Network > Network Profiles > BFD Profile](#)
- ▲ [Network > Network Profiles > QoS](#)

Network > Network Profiles > GlobalProtect IPSec Crypto

Use the **GlobalProtect IPSec Crypto Profiles** page to specify algorithms for authentication and encryption in VPN tunnels between a GlobalProtect gateway and clients. The order in which you add algorithms is the order in which the firewall applies them, and can affect tunnel security and performance. To change the order, select an algorithm and **Move Up** or **Move Down**.



For VPN tunnels between GlobalProtect gateways and satellites (firewalls), see [Network > Network Profiles > IPSec Crypto](#).

GlobalProtect IPSec Crypto Profile Setting	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. If you are not certain of what the VPN peers support, you can add multiple encryption algorithms in top-to-bottom order of most-to-least secure, as follows— aes-256-gcm , aes-128-gcm , and aes-128-cbc . The peers negotiate the strongest algorithm to establish the tunnel.
Authentication	Click Add and select the authentication algorithm to provide data integrity and authenticity protection. Currently, the only option is sha1 . Although the authentication algorithm is required for the profile, this setting only applies to the AES-CBC cipher (aes-128-cbc). If you use an AES-GCM encryption algorithm (aes-256-gcm or aes-128-gcm), the setting is ignored because these ciphers natively provide ESP integrity protection.

Network > Network Profiles > IKE Gateways

Use this page to manage or define a gateway, including the configuration information necessary to perform Internet Key Exchange (IKE) protocol negotiation with a peer gateway. This is the Phase 1 portion of the IKE/IPSec VPN setup.

To manage, configure, restart, or refresh an IKE gateway, see the following:

- [IKE Gateway Management](#)
- [IKE Gateway General Tab](#)
- [IKE Gateway Advanced Options Tab](#)
- [IKE Gateway Restart or Refresh](#)

IKE Gateway Management

The following table describes how to manage your IKE gateways.

Manage IKE Gateways	Description
Add	To create a new IKE gateway, click Add . See IKE Gateway General Tab and IKE Gateway Advanced Options Tab for instructions on configuring the new gateway.
Delete	To delete a gateway, select the gateway and click Delete .
Enable	To enable a gateway that has been disabled, select the gateway and click Enable , which is the default setting for a gateway.
Disable	To disable a gateway, select the gateway and click Disable .

IKE Gateway General Tab

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](#).

IKE Gateway General Setting	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.

IKE Gateway General Setting	Description
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.
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 and enter a value— FQDN (hostname), IP address , KEYID (binary format ID string in HEX), or 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 and enter a value— FQDN (hostname), IP address , KEYID (binary format ID string in HEX), or User FQDN (email address). If no value is specified, the peer's IP address will be used as the Peer Identification value.

IKE Gateway General Setting	Description
Certificate Fields	
Local Certificate	<p>If Certificate is selected as the Authentication type, from the drop-down, select a certificate that is already on the firewall.</p> <p>Alternatively, you can Import a certificate or Generate a new certificate:</p> <p>Import</p> <ul style="list-style-type: none"> • Certificate Name—Enter a name for the certificate you are importing. • Shared—Click if this certificate is to be shared among multiple virtual systems. • Certificate File—Click Browse to navigate to the location where the certificate file is located. Click on the file and select Open. • File Format—Select one of the following: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <p>Generate</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Type—Optionally select additional attribute types from the drop-down to be in the certificate. • Value—Enter a value for the attribute.

IKE Gateway General Setting	Description
HTTP Certificate Exchange	<p>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.</p> <p>If the peer indicates that it too supports Hash and URL, certificates are exchanged through the SHA1 Hash and URL exchange.</p> <p>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.</p>
Local Identification	Identifies how the local peer is identified in the certificate. Choose one of the following types and enter the value— Distinguished Name (Subject), FQDN (hostname), IP address , or User FQDN (email address).
Peer Identification	Identifies how the remote peer is identified in the certificate. Choose one of the following types and enter the value— Distinguished Name (Subject), FQDN (hostname), IP address , or User FQDN (email address).
Peer ID Check	Select Exact or Wildcard . This setting applies to the Peer Identification that is being examined to validate the certificate. Suppose the Peer Identification was a Name equal to domain.com. If you select Exact and name of the certificate in the IKE ID payload is mail.domain2.com, the IKE negotiation will fail. But if you selected Wildcard , any character in the Name string before the wildcard asterisk (*) must match and any character after the wildcard 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 Device > Certificate Management > 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

Select **Network > Network Profiles > IKE Gateways** to configure more advanced settings for an IKE gateway.

IKE Gateway Advanced Option	Description
Enable Passive Mode	Click to have the firewall only respond to IKE connections and never initiate them.
Enable NAT Traversal	Click to have UDP encapsulation used on IKE and UDP protocols, enabling them to pass through intermediate NAT devices. Enable NAT Traversal if Network Address Translation (NAT) is configured on a device between the IPSec VPN terminating points.

IKEv1 Tab

Exchange Mode	Choose auto , aggressive , or main . In auto mode (default), the device can accept both main mode and aggressive mode negotiation requests; however, whenever possible, it initiates negotiation and allows exchanges in main mode. You must configure the peer device with the same exchange mode to allow it to accept negotiation requests initiated from the first device.
IKE Crypto Profile	Select an existing profile, keep the default profile, or create a new profile. The profiles selected for IKEv1 and IKEv2 can differ. For information on IKE Crypto profiles, see Network > Network Profiles > IKE Crypto .
Enable Fragmentation	Click to allow the local gateway to receive fragmented IKE packets. The maximum fragmented packet size is 576 bytes.

IKE Gateway Advanced Option	Description
Dead Peer Detection	Click to enable and enter an interval (2 - 100 seconds) and delay before retrying (2 - 100 seconds). Dead peer detection identifies inactive or unavailable IKE peers and can help restore resources that are lost when a peer is unavailable.
IKEv2 Tab	
IKE Crypto Profile	Select an existing profile, keep the default profile, or create a new profile. The profiles selected for IKEv1 and IKEv2 can differ. For information on IKE Crypto profiles, see Network > Network Profiles > IKE Crypto .
Strict Cookie Validation	Click to enable Strict Cookie Validation on the IKE gateway. <ul style="list-style-type: none"> When you enable Strict Cookie Validation, IKEv2 cookie validation is always enforced; the initiator must send an IKE_SA_INIT containing a cookie. When you disable Strict Cookie Validation (default), the system will check the number of half-open SAs against the global Cookie Activation Threshold, which is a VPN Sessions setting. If the number of half-open SAs exceeds the Cookie Activation Threshold, the initiator must send an IKE_SA_INIT containing a cookie.
Liveness Check	The IKEv2 Liveness Check is always on; all IKEv2 packets serve the purpose of a liveness check. Click this box to have the system send empty informational packets after the peer has been idle for a specified number of seconds (range is 2-100; default is 5). <p>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.</p>

IKE Gateway Restart or Refresh

▲ Network > IPSec Tunnels

Select **Network > IPSec Tunnels** to display status of tunnels. In the second Status column, there is a link to the **IKE Info**. Click the gateway you want to restart or refresh to open the IKE Info page, click one of the entries in the list, and then choose an option:

- **Restart**—Restarts the selected gateway. A restart will disrupt traffic going across the tunnel. The restart behaviors for IKEv1 and IKEv2 are different, as follows:
 - **IKEv1**—You can restart (clear) a Phase 1 SA or Phase 2 SA independently and only that SA is affected.
 - **IKEv2**—Causes all child SAs (IPSec tunnels) to be cleared when the IKEv2 SA is restarted.
If you restart the IKEv2 SA, all underlying IPSec tunnels are also cleared.
If you restart the IPSec Tunnel (child SA) associated with an IKEv2 SA, the restart will not affect the IKEv2 SA.
- **Refresh**—Shows the current IKE SA status.

Network > Network Profiles > IPSec Crypto

Select **Network > Network Profiles > IPSec Crypto** to configure IPSec Crypto profiles that specify protocols and algorithms for authentication and encryption in VPN tunnels based on IPSec SA negotiation (Phase 2).



For VPN tunnels between GlobalProtect gateways and clients, see [Network > Network Profiles > GlobalProtect IPSec Crypto](#).

IPSec Crypto Profile Setting	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: <ul style="list-style-type: none"> 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 Move Up and Move Down to change the order (top to bottom) to the following— aes-256-gcm , aes-256-cbc , aes-192-cbc , aes-128-gcm , aes-128-ccm (the VM-Series firewall doesn't support this option), aes-128-cbc , 3des , and des . You can also select null (no encryption).
Authentication	Click Add and select the desired authentication algorithms. For highest security, use Move Up and Move Down to change the order (top to bottom) to the following— sha512 , sha384 , sha256 , sha1 , md5 . If the IPSec Protocol is ESP , you can also select None (no authentication).
DH Group	Select the Diffie-Hellman (DH) group for IKE—group1 , group2 , group5 , group14 , group19 , or group20 . For highest security, choose the group with the highest number. If you don't want to renew the key that the firewall creates during IKE phase 1, select no-pfs (no perfect forward secrecy)—the firewall reuses the current key for the IPSec security association (SA) negotiations.
Lifetime	Select units and enter the length of time (default is one hour) that the negotiated key will stay effective.
Lifesize	Select optional units and enter the amount of data that the key can use for encryption.

Network > Network Profiles > IKE Crypto

Use the **IKE Crypto Profiles** page to specify protocols and algorithms for identification, authentication, and encryption (IKEv1 or IKEv2, Phase 1).

To change the order in which an algorithm or group is listed, select the item and then click **Move Up** or **Move Down**. The order determines the first choice when settings are negotiated with a remote peer. The setting at the top of the list is attempted first, continuing down the list until an attempt is successful.

IKE Crypto Profile Setting	Description
Name	Enter a name for the profile.
DH Group	Specify the priority for Diffie-Hellman (DH) groups. Click Add and select groups— group1 , group2 , group5 , group14 , group19 , or group20 . For highest security, select an item and then click Move Up or Move Down to move the groups with higher numeric identifiers to the top of the list. For example, move group14 above group2 .
Authentication	Specify the priority for hash algorithms. Click Add and select algorithms. For highest security, select an item and then click Move Up or Move Down to change the order (top to bottom) to the following— sha512 , sha384 , sha256 , sha1 , md5 .
Encryption	Select the appropriate Encapsulating Security Payload (ESP) authentication options. Click Add and select algorithms. For highest security, select an item and then click Move Up or Move Down to change the order (top to bottom) to the following— aes-256-cbc , aes-192-cbc , aes-128-cbc , 3des , des .
Key Lifetime	Select unit of time and enter the length of time that the negotiated IKE Phase 1 key will be effective (default is 8 hours). <ul style="list-style-type: none"> • 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.

Network > Network Profiles > Interface Mgmt

An Interface Management profile protects the firewall from unauthorized access by defining the services and IP addresses that a firewall interface permits. You can assign an Interface Management profile to Layer 3 Ethernet interfaces (including subinterfaces) and to logical interfaces (aggregate group, VLAN, loopback, and tunnel interfaces). To assign an Interface Management profile, see [Network > Interfaces](#).

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.
Permitted Services	<ul style="list-style-type: none"> • Ping—Use to test connectivity with external services. For example, you can ping the interface to verify it can receive PAN-OS software and content updates from the Palo Alto Networks Update Server. • Telnet—Use to access the firewall CLI. Telnet uses plaintext, which is not as secure as SSH. Therefore, as a best practice, enable SSH instead of Telnet for management traffic on the interface. • SSH—Use for secure access to the firewall CLI. • HTTP—Use to access the firewall web interface. HTTP uses plaintext, which is not as secure as HTTPS. Therefore, as a best practice, enable HTTPS instead of HTTP for management traffic on the interface. • HTTP OCSP—Use to configure the firewall as an Online Certificate Status Protocol (OCSP) responder. For details, see Device > Certificate Management > OCSP Responder. • HTTPS—Use for secure access to the firewall web interface. • SNMP—Use to process firewall statistics queries from an SNMP manager. For details, see Enable SNMP Monitoring. • Response Pages—Use this option to configure response pages: <ul style="list-style-type: none"> • Captive Portal—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. For details, see Device > User Identification > Captive Portal Settings. • URL Admin Override—For details, see Device > Setup > Content-ID. • User-ID—Use to Enable Redistribution of User Mappings Among Firewalls. • User-ID Syslog Listener-SSL—Use to allow the PAN-OS integrated User-ID agent to collect syslog messages over SSL. For details, see Configure Access to Monitored Servers. • User-ID Syslog Listener-UDP—Use to allow the PAN-OS integrated User-ID agent to collect syslog messages over UDP. For details, see Configure Access to Monitored Servers.
Permitted IP Addresses	Enter the list of IPv4 or IPv6 addresses from which the interface allows access.

Network > Network Profiles > Monitor

A monitor profile is used to monitor IPSec tunnels and to monitor a next-hop device for policy-based forwarding (PBF) rules. In both cases, the monitor profile is used to specify an action to take when a resource (IPSec tunnel or next-hop device) becomes unavailable. Monitor profiles are optional, but can be very useful for maintaining connectivity between sites and to ensure that PBF rules are maintained. The following settings are used to configure a monitor profile.

Field	Description
Name	Enter a name to identify the monitor profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Action	<p>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.</p> <ul style="list-style-type: none"> • 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. <p>In both cases, the firewall tries to negotiate new IPSec keys to accelerate the recovery.</p>
Interval	Specify the time between heartbeats (range is 2-10; default is 3).
Threshold	Specify the number of heartbeats to be lost before the firewall takes the specified action (range is 2-10; default is 5).

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 is not designed to protect a specific end host or traffic going to a particular destination zone.

To augment zone protection capabilities on the firewall, use the DoS protection rulebase to match on a specific zone, interface, IP address, or user.



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

To create a zone protection profile, click **Add** and specify the first two settings.

Zone Protection Profile Setting	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	(Optional) Enter a description for the zone protection profile.

Continue to create a zone protection profile by configuring any combination of settings based on what types of protection your zone needs:

- **Flood Protection**—See [Configuring Flood Protection](#).
- **Reconnaissance Profile**—See [Configuring Reconnaissance Protection](#).
- **Packet Based Attack Protection**—See [Configuring Packet Based Attack Protection](#).
 - [Configuring the IP Drop tab](#)
 - [Configuring the TCP Drop tab](#)
 - [Configuring the ICMP Drop Tab](#)
 - [Configuring the IPv6 Drop Tab](#)
 - [Configuring the ICMPv6 Drop tab](#)



If you have an environment with multiple virtual systems and you enable 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

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

- SYN cookies
- IP fragmentation
- ICMPv6

To enable IP fragmentation and ICMPv6 protection, 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

Flood Protection Setting	Description
Flood Protection Thresholds - SYN Flood	
Action	<p>Select the action to take in response to a SYN flood attack.</p> <ul style="list-style-type: none"> • Random Early Drop—Causes SYN packets to be dropped to mitigate a flood attack: <ul style="list-style-type: none"> • 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. You can view alarms on the Dashboard (refer to Dashboard) and in the threat log (refer to Monitor > Packet Capture).
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 the zone will receive per second. Any number of packets exceeding the maximum in a second will be dropped.
Flood Protection Thresholds - ICMP Flood	
Alert (packets/sec)	Enter the number of ICMP echo requests (pings) received by the zone (in a 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 the zone will receive per second. Any number of packets exceeding the maximum in a second will be dropped.
Flood Protection Thresholds - ICMPv6	
Alert (packets/sec)	Enter the number of ICMPv6 echo requests (pings) received by the zone (in a second) that triggers an attack alarm.
Activate (packets/sec)	Enter the number of ICMPv6 packets received by the zone (in a second) 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 the zone will receive per second. Any number of packets exceeding the maximum in a second will be dropped.

Flood Protection Setting	Description
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 the zone will receive per second. Any number of packets exceeding the maximum in a second will be dropped.
Flood Protection Thresholds - Other IP	
Alert (packets/sec)	Enter the number of other IP packets (non-TCP, non-ICMP, non-ICMPv6, and non-UDP packets) received by the zone (in a second) that triggers an attack alarm.
Activate (packets/sec)	Enter the number of other IP packets (non-TCP, non-ICMP, non-ICMPv6, and non-UDP packets) received by the zone (in a second) that triggers random dropping of other IP packets. The response is disabled when the number of other IP packets drops below the threshold. Any number of packets exceeding the maximum will be dropped.
Maximum (packets/sec)	Enter the maximum number of other IP packets (non-TCP, non-ICMP, non-ICMPv6, and non-UDP packets) the zone will receive per second. Any number of packets exceeding the maximum in a second will be dropped.

Configuring Reconnaissance Protection

▲ Network > Network Profiles > Zone Protection > Reconnaissance Protection

The following table describes reconnaissance protection settings for zone protection.

Zone Protection Field	Description
TCP Port Scan	Enable configures the profile to enable protection against TCP port scans.
UDP Port Scan	Enable configures the profile to enable protection against UDP port scans.
Host Sweep	Enable configures the profile to enable protection against host sweeps.

Zone Protection Field	Description
Action	Action that the system will take in response to the corresponding reconnaissance attempt: <ul style="list-style-type: none"> Allow—Permits the port scan or host sweep reconnaissance. Alert—Generates an alert for each port scan or host sweep that matches the threshold within the specified time interval (the default action). Block—Drops all subsequent packets from the source to the destination for the remainder of the specified time interval. Block IP—Drops all subsequent packets for the specified Duration, in seconds (range is 1-3,600). Track By determines whether to block source or source-and-destination traffic. For example, block attempts above the threshold number per interval that are from a single source (more stringent), or block attempts that have a source and destination pair (less stringent).
Interval (sec)	Time interval (in seconds) for TCP or UDP port scan detection (range is 2-65,535; default is 2). Time interval (in seconds) for host sweep detection (range is 2-65,535; default is 10).
Threshold (events)	Number of scanned port events or host sweep events within the specified time interval that triggers the Action (range is 2-65,535; default is 100).

Configuring Packet Based Attack Protection

▲ Network > Network Profiles > Zone Protection > Packet Based Attack Protection

You can configure Packet Based Attack protection by dropping types of packets with various characteristics:

- **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 Drop**—See [Configuring the ICMPv6 Drop tab](#).

Configuring the IP Drop tab

To instruct the firewall what to do with certain IP packets it received in the zone, specify the following settings.

Packet Based Attack Protection Setting	Description
IP Drop tab	
Spoofed IP address	Discard packets with a spoofed IP address.

Packet Based Attack Protection Setting	Description
Strict IP Address Check	<p>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, a link-local address, an unspecified address, or is reserved for future use.</p> <p>For a firewall in Common Criteria (CC) mode, you can enable logging for discarded packets. On the firewall web interface, select Device > Log Settings. In the Manage Logs section, select Selective Audit and enable Packet Drop Logging.</p>
Fragmented traffic	Discard 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 RFCs 791, 1108, 1393, and 2113.

Configuring the TCP Drop tab

To instruct the firewall what to do with certain TCP packets it received in the zone, specify the following settings.

TCP Drop Setting	Description
Mismatched overlapping TCP segment	<p>Report an overlap mismatch and drop the packet when segment data does not match in these scenarios:</p> <ul style="list-style-type: none"> • The segment is within another segment. • The segment overlaps with part of another segment. • The segment covers another segment. <p>This protection mechanism uses sequence numbers to determine where packets reside within the TCP data stream.</p>

TCP Drop Setting	Description
Split Handshake	<p>Prevent 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.</p> <p>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.</p>
Reject Non-SYN TCP	<p>Determine whether to reject the packet if the first packet for the TCP session setup is not a SYN packet:</p> <ul style="list-style-type: none"> • 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	<p>Determine whether to drop or bypass packets that contain out-of-sync ACKs or out-of-window sequence numbers:</p> <ul style="list-style-type: none"> • 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	Determine whether the packet has a TCP timestamp in the header and, if it does, strip the timestamp from the header.

Configuring the ICMP Drop Tab

To instruct the firewall what to do with certain ICMP packets it received in the zone, specify the following settings.

ICMP Drop Setting	Description
ICMP Ping ID 0	Discard packets if the ICMP ping packet has an identifier value of 0.
ICMP Fragment	Discard packets that consist of ICMP fragments.
ICMP Large Packet (>1024)	Discard ICMP packets that are larger than 1024 bytes.
Discard ICMP embedded with error message	Discard ICMP packets that are embedded with an error message.
Suppress ICMP TTL Expired Error	Stop sending ICMP TTL expired messages.
Suppress ICMP Frag Needed	Stop sending ICMP fragmentation needed messages in response to packets that exceed the interface MTU and have the do not fragment (DF) bit set. This setting will interfere with the PMTUD process performed by hosts behind the firewall.

Configuring the IPv6 Drop Tab

To instruct the firewall what to do with certain IPv6 packets it received in the zone, specify the following settings.

IPv6 Drop Setting	Description
Type 0 Routing Heading	Discard IPv6 packets containing a Type 0 routing header. See RFC 5095 for Type 0 routing header information.
IPv4 compatible address	Discard IPv6 packets that are defined as an RFC 4291 IPv4-Compatible IPv6 address.
Anycast source address	Discard IPv6 packets that contain an anycast source address.
Needless fragment header	Discard IPv6 packets with the last fragment flag (M=0) and offset of zero.
MTU in ICMP 'Packet Too Big' less than 1280 bytes	Discard IPv6 packets that contain a Packet Too Big ICMPv6 message when the maximum transmission unit (MTU) is less than 1,280 bytes.
Hop-by-Hop extension	Discard IPv6 packets that contain the Hop-by-Hop Options extension header.
Routing extension	Discard IPv6 packets that contain the Routing extension header, which directs packets to one or more intermediate nodes on its way to its destination.
Destination extension	Discard IPv6 packets that contain the Destination Options extension, which contains options intended only for the destination of the packet.
Invalid IPv6 options in extension header	Discard IPv6 packets that contain invalid IPv6 options in an extension header.
Non-zero reserved field	Discard IPv6 packets that have a header with a reserved field not set to zero.

Configuring the ICMPv6 Drop tab

To instruct the firewall what to do with certain ICMPv6 packets it received in the zone, specify the following settings.

ICMPv6 Drop Setting	Description
ICMPv6 destination unreachable - require explicit security rule match	Require an explicit security policy match for Destination Unreachable ICMPv6 messages, even when the message is associated with an existing session.
ICMPv6 packet too big - require explicit security rule match	Require an explicit security policy match for Packet Too Big ICMPv6 messages, even when the message is associated with an existing session.
ICMPv6 time exceeded - require explicit security rule match	Require an explicit security policy match for Time Exceeded ICMPv6 messages, even when the message is associated with an existing session.
ICMPv6 parameter problem - require explicit security rule match	Require an explicit security policy match for Parameter Problem ICMPv6 messages, even when the message is associated with an existing session.
ICMPv6 redirect - require explicit security rule match	Require an explicit security policy match for Redirect Message ICMPv6 messages, even when the message is associated with an existing session.

Network > Network Profiles > LLDP Profile

A Link Layer Discovery Protocol (LLDP) profile is the way in which you configure the LLDP mode of the firewall, enable syslog and SNMP notifications, and configure the optional Type-Length-Values (TLVs) you want transmitted to LLDP peers. After configuring the LLDP profile, you assign the profile to one or more interfaces.

Learn more about [LLDP](#), including how to configure and monitor LLDP.

LLDP Profile Setting	Description
Name	Specify a name for the LLDP profile.
Mode	Select the mode in which LLDP will function— transmit-receive , transmit-only , or receive-only .
SNMP Syslog Notification	Enables SNMP trap and syslog notifications, which will occur at the global Notification Interval . If enabled, the firewall will send both an SNMP trap and a syslog event as configured in the Device > Log Settings > System > SNMP Trap Profile and Syslog Profile .
Port Description	Enables the ifAlias object of the firewall to be sent in the Port Description TLV.
System Name	Enables the sysName object of the firewall to be sent in the System Name TLV.
System Description	Enables the sysDescr object of the firewall to be sent in the System Description TLV.
System Capabilities	<p>Enables the deployment mode (L3, L2, or virtual wire) of the interface to be sent, via the following mapping, in the System Capabilities TLV.</p> <ul style="list-style-type: none"> • 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). <p>SNMP MIB will combine capabilities configured on interfaces into a single entry.</p>
Management Address	Enables the Management Address to be sent in the Management Address TLV. You can enter up to four management addresses, which are sent in the order they are specified. To change the order, click Move Up or Move Down .
Name	Specify a name for the Management Address.
Interface	Select an interface whose IP address will be the Management Address. If you select None , you can enter an IP address in the field next to the IPv4 or IPv6 selection.
IP Choice	Select IPv4 or IPv6 , and in the adjacent field, select or enter the IP address to be transmitted as the Management Address. At least one management address is required if Management Address TLV is enabled. If no management IP address is configured, the system uses the MAC address of the transmitting interface as the management address transmitted.

Network > Network Profiles > BFD Profile

Bidirectional Forwarding Detection (BFD) enables extremely fast detection of a link failure, which accelerates failover to a different route.

What do you want to know?	See:
What is BFD?	BFD Overview
What fields are available to create a BFD profile?	Building Blocks of a BFD Profile
View BFD status for a virtual router.	View BFD Summary and Details
Looking for more?	Learn more about and configure BFD . Configure BFD for: <ul style="list-style-type: none"> • Static Routes • BGP • OSPF • OSPFv3 • RIP

BFD Overview

BFD is a protocol that recognizes a failure in the bidirectional path between two forwarding engines, such as interfaces, data links, or the actual forwarding engines. In the PAN-OS implementation, one of the forwarding engines is an interface on the firewall and the other is an adjacent configured BFD peer. The BFD failure detection between two engines is extremely fast, providing faster failover than could be achieved by link monitoring or frequent dynamic routing health checks, such as Hello packets or heartbeats.

After BFD detects a failure, it notifies the routing protocol to switch to an alternate path to the peer. If BFD is configured for a static route, the firewall removes the affected routes from the RIB and FIB tables.

BFD is supported on the following interface types—physical Ethernet, AE, VLAN, tunnel (Site-to-Site VPN and LVPN), and subinterfaces of Layer 3 interfaces. For each static route or dynamic routing protocol, you can enable or disable BFD, select the default BFD profile, or configure a BFD profile.

Building Blocks of a BFD Profile

▲ Network > Network Profiles > BFD Profile

You can enable BFD for a static route or dynamic routing protocol by applying the default BFD profile or a BFD profile that you create. The default profile uses the default BFD settings and cannot be changed. You can **Add** a new BFD profile and specify the following information.

BFD Profile Setting	Description
Name	Name of the BFD profile (up to 31 characters). The name is case-sensitive and must be unique on the firewall. Use only letters, numbers, spaces, hyphens, and underscores.

BFD Profile Setting	Description
Mode	Mode in which BFD operates: <ul style="list-style-type: none">• Active—BFD initiates sending control packets (default). At least one of the BFD peers must be active; they can both be active.• Passive—BFD waits for the peer to send control packets and responds as required.
Desired Minimum Tx Interval (ms)	Minimum interval (in milliseconds) at which you want the BFD protocol to send BFD control packets. Minimum value on PA-7000/PA-5000 Series is 50; minimum on PA-3000 Series is 100; minimum on VM-Series is 200 (maximum value is 2,000; default is 1,000).  If you have multiple protocols that use different BFD profiles on the same interface, configure the BFD profiles with the same Desired Minimum Tx Interval .
Required Minimum Rx Interval (ms)	Minimum interval (in milliseconds) at which BFD can receive BFD control packets. Minimum value on PA-7000/PA-5000 Series is 50; minimum on PA-3000 Series is 100; minimum on VM-Series is 200 (maximum value is 2,000; default is 1,000).
Detection Time Multiplier	The transmit interval (negotiated from the Desired Minimum Tx Interval) multiplied by the Detection Time Multiplier equals the detection time. If BFD does not receive a BFD control packet from its peer before the detection time expires, a failure has occurred (range is 2-50; default is 3).
Hold Time (ms)	Delay (in milliseconds) after a link comes up before the firewall transmits BFD control packets. Hold Time applies to BFD Active mode only. If the firewall receives BFD control packets during the Hold Time , it ignores them (range is 0-120,000; default is 0). The default setting of 0 means no transmit Hold Time is used; the firewall sends and receives BFD control packets immediately after the link is established.
Enable Multihop	Enables BFD over multiple hops. Applies to BGP implementation only.
Minimum Rx TTL	Minimum Time-to-Live value (number of hops) BFD will accept (receive) when it supports multihop BFD. Applies to BGP implementation only (range is 1-254; there is no default).

View BFD Summary and Details

▲ Network > Virtual Routers

The following table describes how to view BFD information.

View BFD Information	Description
View a BFD summary.	Select Network > Virtual Routers and in the row of the virtual router you are interested in, click More Runtime Stats . Select the BFD Summary Information tab.
View BFD details.	Select details in the row of the interface you are interested in to view BFD Details .

Network > Network Profiles > QoS

Add a QoS profile to define the bandwidth limits and priority for up to eight classes of service. You can set both guaranteed and maximum bandwidth limits for individual classes and for the collective classes. Priorities determine how traffic is treated in the presence of contention.

To fully enable the firewall to provide QoS, you must also:

- Define the traffic that you want to receive QoS treatment (select **Policies > QoS** to add or modify a QoS policy).
- Enable QoS on an interface (select **Network > QoS**).

See [Quality of Service](#) for complete QoS workflows, concepts, and use cases.

QoS Profile Setting	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	<p>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 enabled with QoS. See Network > QoS.</p> <p> Though this is not a required field, it is recommended to always define the Egress Max value for a QoS profile.</p>
Egress Guaranteed	Enter the bandwidth that is guaranteed for this profile (Mbps). When the egress guaranteed bandwidth is exceeded, the firewall passes traffic on a best-effort basis.
Classes	<p>Click Add to specify how to treat individual QoS classes. You can select one or more classes to configure:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • real-time • high • medium • low <p>When contention occurs, traffic that is assigned a lower priority is dropped. Real-time priority uses its own separate queue.</p> <ul style="list-style-type: none"> • 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. <p> Though this is not a required field, it is recommended to always define the Egress Max value for a QoS profile.</p> <ul style="list-style-type: none"> • Egress Guaranteed—Click and enter the guaranteed bandwidth (Mbps) for this class. Guaranteed bandwidth assigned to a class is not reserved for that class—bandwidth that is unused continues to remain available to all traffic. However, when the egress guaranteed bandwidth for a traffic class is exceeded, the firewall passes that traffic on a best-effort basis.



Device

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

- ▲ [Device > Setup](#)
- ▲ [Device > High Availability](#)
- ▲ [Device > Config Audit](#)
- ▲ [Device > Password Profiles](#)
- ▲ [Device > Administrators](#)
- ▲ [Device > Admin Roles](#)
- ▲ [Device > Access Domain](#)
- ▲ [Device > Authentication Sequence](#)
- ▲ [Device > Authentication Profile](#)
- ▲ [Device > Authentication Sequence](#)
- ▲ [Device > User Identification](#)
- ▲ [Device > VM Information Sources](#)
- ▲ [Device > Virtual Systems](#)
- ▲ [Device > Shared Gateways](#)
- ▲ [Device > Certificate Management](#)
- ▲ [Device > Response Pages](#)
- ▲ [Device > Log Settings](#)
- ▲ [Device > Server Profiles](#)
- ▲ [Device > Local User Database > Users](#)
- ▲ [Device > Local User Database > User Groups](#)
- ▲ [Device > Scheduled Log Export](#)
- ▲ [Device > Software](#)
- ▲ [Device > GlobalProtect Client](#)
- ▲ [Device > Dynamic Updates](#)
- ▲ [Device > Licenses](#)
- ▲ [Device > Support](#)
- ▲ [Device > Master Key and Diagnostics](#)

Device > Setup

- ▲ [Device > Setup > Management](#)
- ▲ [Device > Setup > Operations](#)
- ▲ [Device > Setup > HSM](#)
- ▲ [Device > Setup > Services](#)
- ▲ [Device > Setup > Content-ID](#)
- ▲ [Device > Setup > WildFire](#)
- ▲ [Device > Setup > Session](#)

Device > Setup > Management

- ▲ Device > Setup > Management
- ▲ Panorama > Setup > Management

On a firewall, select **Device > Setup > Management** to configure management settings.

On Panorama™, select **Device > Setup > Management** to configure firewalls that you manage with Panorama templates. Select **Panorama > Setup > Management** to configure settings for Panorama.

The following management settings 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 for its connection to the firewalls)
- [Management Interface Settings](#)
- [Eth1 Interface Settings \(Panorama only\)](#)
- [Eth2 Interface Settings \(Panorama only\)](#)
- [Logging and Reporting Settings](#)
- [Banners and Messages](#)
- [Minimum Password Complexity](#)
- [AutoFocus](#)

The following table describes Panorama general settings.

Item	Description
General Settings	
Hostname	<p>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. If you don't enter a value, PAN-OS uses the platform model (for example, PA-5050_2) as the default.</p> <p> Optionally, you can configure the firewall to use a hostname that a DHCP server provides. See Accept DHCP server-provided Hostname.</p>
Domain	<p>Enter the Fully Qualified Domain Name (FQDN) of the firewall (up to 31 characters).</p> <p>If you don't enter a value, PAN-OS uses the platform model (for example, PA-5050_2) as the default.</p> <p> Optionally, you can configure the firewall to use a domain that a DHCP server provides. See Accept DHCP server-provided Domain.</p>
Accept DHCP server-provided Hostname (Firewall only)	<p>(Applies only when the Management Interface IP Type is DHCP Client.)</p> <p>Select this option to have the management interface accept the hostname it receives from the DHCP server. The hostname from the server (if valid) overwrites any value specified in the Hostname field.</p>

Item	Description
Accept DHCP server-provided Domain (Firewall only)	(Applies only when the Management Interface IP Type is DHCP Client.) Select this option to have the management interface accept the domain (DNS suffix) it receives from the DHCP server. The domain from the server overwrites any value specified in the Domain field.
Login Banner	Enter text (up to 3,200 characters) to display on the web interface login page below the Name and Password fields.
Force Admins to Acknowledge Login Banner	Select this option to display and force administrators to select the I Accept and Acknowledge the Statement Below option above the login banner on the login page; administrators must acknowledge the message before they can Login .
SSL/TLS Service Profile	Assign an existing SSL/TLS Service profile or create a new one to specify a certificate and the allowed protocols for securing inbound management traffic (see Device > Certificate Management > SSL/TLS Service Profile). The firewall or Panorama uses this certificate to authenticate to administrators who access the web interface through the management (MGT) interface or through any other interface that supports HTTP/HTTPS management traffic (see Network > Network Profiles > Interface Mgmt). If you select None (default), the firewall or Panorama uses a predefined certificate.  Don't use the predefined certificate. For better security, we recommend that you assign an SSL/TLS Service profile associated with a certificate that the client systems of administrators trust. To ensure trust, the certificate must be signed by a certificate authority (CA) certificate that is in the trusted root certificate store of the client systems.
Time Zone	Select the time zone of the firewall.
Locale	Select a language for PDF reports from the drop-down. See Monitor > PDF Reports > Manage PDF Summary . Even if you have a specific language preference set for the web interface, PDF reports will use the language specified for Locale .
Time	Set the date and time on the firewall: <ul style="list-style-type: none">• 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).  You can also define an NTP server from Device > Setup > Services .
Serial Number (Panorama virtual appliances only)	Enter the serial number for Panorama. Find the serial number in the order fulfillment email that you received from Palo Alto Networks.
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 this option to automatically apply a commit lock when you change the candidate configuration. For more information, see Lock Configurations .
Certificate Expiration Check	Instruct the firewall to create warning messages when on-box certificates near their expiration dates.

Item	Description
Multi Virtual System Capability	<p>Enables the use of multiple virtual systems on firewalls that support this feature (see Device > Virtual Systems).</p>  <p>To enable multiple virtual systems on a PA-5060 firewall or PA-7000 Series firewall, the firewall policies must reference no more than 640 distinct user groups. If necessary, reduce the number of referenced user groups. Then, after you enable and add multiple virtual systems, the policies can then reference another 640 user groups for each additional virtual system.</p>
URL Filtering Database (Panorama only)	<p>Select a URL Filtering vendor for use with Panorama—brightcloud or paloaltonetworks (PAN-DB).</p>
Use Hypervisor Assigned MAC Addresses (VM-Series firewalls only)	<p>Select this option to have the VM-Series firewall use the MAC address that the hypervisor assigned, instead of generating a MAC address using the PAN-OS® custom schema.</p> <p>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.</p>
Authentication Settings	
Authentication Profile	<p>Select the authentication profile (or sequence) that the firewall uses to authenticate administrators who have external accounts (accounts that are not defined on the firewall). 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 firewall requests authentication information (including the administrator role) from the RADIUS server.</p> <p>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 firewall and the RADIUS server. Refer to the RADIUS server software documentation for instructions on where to install the file.</p> <p>If you select None, the firewall won't authenticate external administrators; they cannot log in.</p> <p>For details, see Device > Authentication Profile and Device > Server Profiles > RADIUS.</p>  <p>If an administrator is local, the firewall uses the authentication profile associated with the administrator account for authentication (see Device > Administrators).</p>
Certificate Profile	<p>Select a certificate profile to verify the client certificates of administrators who are configured for certificate-based access to the firewall web interface. For instructions on configuring certificate profiles, see Device > Certificate Management > Certificate Profile.</p>

Item	Description
Idle Timeout	<p>Enter the number of minutes that must pass without administrator activity during a firewall web interface or CLI session before the firewall automatically logs out the administrator (range is 0–1,440; default is 60). A value of 0 means that inactivity does not trigger the automatic logout.</p>  <p>Both manual and automatic refreshing of web interface pages (such as the Dashboard tab and System Alarms dialog) reset the Idle Timeout counter. To enable the firewall to enforce the timeout when you are on a page that supports automatic refreshing, set the refresh interval to Manual or to a value higher than the Idle Timeout. You can also disable Auto Refresh in the ACC tab.</p>
Failed Attempts	<p>Enter the number of failed login attempts (range is 0–10) that the firewall allows for the web interface and CLI before locking out the administrator account. A value of 0 (default) specifies unlimited login attempts. Limiting login attempts can help protect the firewall from brute force attacks.</p>  <p>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.</p>
Lockout Time	<p>Enter the number of minutes (range is 0–60) for which the firewall locks out an administrator from access to the web interface and CLI after reaching the Failed Attempts limit. A value of 0 (default) means the lockout applies until another administrator manually unlocks the account.</p>  <p>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.</p>

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](#).



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).

Item	Description
Disable/Enable Panorama Policy and Objects	<p>This option displays when you edit the Panorama Settings on a firewall (not in a template on Panorama).</p> <p>Disable Panorama Policy and Objects to disable the propagation of device group policies and objects to the firewall. By default, this action also removes those policies and objects from the firewall. To keep a local copy of the device group policies and objects on the firewall, in the dialog that opens when you click this option, select Import Panorama Policy and Objects before disabling. After you perform a commit, the policies and objects become part of the firewall configuration and Panorama no longer manages them.</p> <p>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.</p> <p>To revert firewall policy and object management to Panorama, click Enable Panorama Policy and Objects.</p>
Disable/Enable Device and Network Template	<p>This option displays only when you edit the Panorama Settings on a firewall (not in a template on Panorama).</p> <p>Disable Device and Network Template to disable 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 select this option, select Import Device and Network Templates before disabling. After you perform a commit, the template information becomes part of the firewall configuration and Panorama no longer manages that information.</p> <p>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.</p> <p>To configure the firewall to accept templates again, click Enable Device and Network Templates.</p>

Panorama Settings: Panorama > Setup > Management

If you use Panorama to manage firewalls, configure the following settings on Panorama. These settings determine timeouts and SSL message attempts for the connections from Panorama to managed firewalls, as well as object sharing parameters.

You must also configure Panorama connection settings on the firewall, or in a template on Panorama. See [Panorama Settings: Device > Setup > Management](#).



The firewall uses an SSL connection with 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).

Item	Description
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 option to share all Panorama shared objects and device-group-specific objects with managed firewalls. This setting is enabled by default. If you clear this option, 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.
Objects defined in ancestors will take higher precedence	Select this option 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. Likewise, this option causes the value of a shared object to override the values of objects of the same type and name in device groups. 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. Likewise, disabling this option causes the value of a device group object to override the value of shared object of the same type and name. Selecting this option displays the Find Overridden Objects link.
Find Overridden Objects	Click this link to list any <i>shadowed</i> objects. A shadowed object is an object in the Shared location that has the same name but a different value in a device group. The link displays only if you select Objects defined in ancestors will take higher precedence .

Management Interface Settings

This interface applies to the firewall, Panorama M-Series appliance, and 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. Specify the **Netmask** subnet (IPv4) or **IPv6 Address/Prefix Length** (IPv6) subnet. The Panorama virtual appliance does not support separate interfaces.

To complete the configuration of the MGT interface, you must specify the IP address, the netmask (for IPv4) or prefix length (for IPv6), and the default gateway. If you commit a partial configuration (for example, you might omit the default gateway), you can only access the firewall or Panorama through the console port for future configuration changes. We recommend that you always commit a complete configuration.



For firewall management, you can optionally [Network > Interfaces > Loopback](#) instead of using the management interface.

Item	Description
Type (Firewall only)	<p>Select one:</p> <ul style="list-style-type: none"> • Static—Requires you to enter the IP Address (IPv4), Netmask (IPv4), and Default Gateway manually. • DHCP Client—Configures the MGT interface as a DHCP client so that the firewall can send DHCP Discover or Request messages to find a DHCP server. The server responds by providing an IP address (IPv4), netmask (IPv4), and default gateway for the MGT interface. DHCP on the MGT interface is turned off by default for the VM-Series firewall (except for the VM-Series firewall in AWS and Azure). If you select DHCP Client, optionally select either or both of the following Client Options: <ul style="list-style-type: none"> • Send Hostname—Causes the management interface to send its hostname to the DHCP server as part of DHCP Option 12. • Send Client ID—Causes the management interface to send its client identifier as part of DHCP Option 61. <p>If you select DHCP Client, optionally click Show DHCP Client Runtime Info to view the dynamic IP interface status:</p> <ul style="list-style-type: none"> • Interface—Indicates management (MGT) interface. • IP Address—IP address of the MGT interface. • Netmask—Subnet mask for the IP address, indicating which bits are network or subnetwork and which are host. • Gateway—Default gateway for traffic leaving the MGT interface. • Primary/Secondary NTP—IP address of up to two NTP servers serving the MGT interface. If the DHCP Server returns NTP server addresses, the firewall considers them only if you did not manually configure NTP server addresses. If you manually configured NTP server addresses, the firewall does not overwrite them with those from the DHCP server. • Lease Time—Number of days, hours, minutes, and seconds that the DHCP IP address is assigned. • Expiry Time—Year/Month/Day, Hours/Minutes/Seconds, and time zone, indicating when DHCP lease will expire. • DHCP Server—IP address of the DHCP Server responding to management interface DHCP Client. • Domain—Name of domain to which the MGT interface belongs. • DNS Server—IP address of up to two DNS servers serving the MGT interface. If the DHCP Server returns DNS server addresses, the firewall considers them only if you did not manually configure DNS server addresses. If you manually configured DNS server addresses, the firewall does not overwrite them with those from the DHCP server. <p> Optionally, you can Renew the DHCP lease for the IP address assigned to the MGT interface. Otherwise, Close the window.</p>
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 firewall 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).

Item	Description
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 firewall or Panorama determine the interface speed.  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 576–1,500; default is 1,500).
Services	Select the services you want to enable on the MGT interface: <ul style="list-style-type: none"> Ping—Use to test connectivity with external services. For example, you can ping the MGT interface to verify it can receive PAN-OS software and content updates from the Palo Alto Networks Update Server. In a high availability (HA) deployment, HA peers use ping to exchange heartbeat backup information. Telnet—Use to access the firewall CLI. Telnet uses plaintext, which is not as secure as SSH. Therefore, as a best practice, enable SSH instead of Telnet for management traffic on the interface. SSH—Use for secure access to the firewall CLI. HTTP—Use to access the firewall web interface. HTTP uses plaintext, which is not as secure as HTTPS. Therefore, as a best practice, enable HTTPS instead of HTTP for management traffic on the interface. HTTP OCSP—Use to configure the firewall as an Online Certificate Status Protocol (OCSP) responder. For details, see Device > Certificate Management > OCSP Responder. HTTPS—Use for secure access to the firewall web interface. SNMP—Use to process firewall statistics queries from an SNMP manager. For details, see Enable SNMP Monitoring. Response Pages—Use to enable response pages: <ul style="list-style-type: none"> Captive Portal—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. For details, see Device > User Identification > Captive Portal Settings. URL Admin Override—for details, see Device > Setup > Content-ID. User-ID—Use to Enable Redistribution of User Mappings Among Firewalls. User-ID Syslog Listener-SSL—Use to enable the PAN-OS integrated User-ID™ agent to collect syslog messages over SSL. For details, see Configure Access to Monitored Servers. User-ID Syslog Listener-UDP—Use to enable the PAN-OS integrated User-ID agent to collect syslog messages over UDP. For details, see Configure Access to Monitored Servers.

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 addresses of all managed firewalls so that they can connect and forward logs to Panorama and 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).	
 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 option 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.  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 576–1,500; default is 1,500).
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).	
 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 option to enable the Eth2 interface.
IP Address (IPv4)	If your network uses IPv4, assign an IPv4 address to the Eth2 interface.

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.  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 576–1,500; default is 1,500).
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.

Item	Description
Logging and Reporting Settings Use this section to modify: <ul style="list-style-type: none"> Expiration periods and storage quotas for the following logs and reports. The settings are synchronized across high availability pairs: <ul style="list-style-type: none"> 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 Panorama > Collector Groups. Attributes for calculating and exporting user activity reports. Predefined reports created on the firewall/Panorama. 	Logging and Reporting Settings Use this section to modify: <ul style="list-style-type: none"> Expiration periods and storage quotas for the following logs and reports. The settings are synchronized across high availability pairs: <ul style="list-style-type: none"> 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 Panorama > Collector Groups. Attributes for calculating and exporting user activity reports. Predefined reports created on the firewall/Panorama.
Log Storage tab (Panorama management server and all firewall platforms except PA-7000 Series firewalls)  Panorama displays this tab if you edit the Logging and Reporting Settings on the Panorama > Setup > Management page. If you use a Panorama template to configure the settings for firewalls (Device > Setup > Management), see Log Card Storage and Management Card Storage tabs .	For each log type, specify: <ul style="list-style-type: none"> 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 firewall or Panorama automatically deletes logs that exceed the specified period. By default, no expiration period is set, which means logs never expire. <p>The firewall or Panorama evaluates logs as it creates them and deletes logs that exceed the expiration period or quota size.</p>  Weekly summary logs can age beyond the threshold before the next deletion if they reach the expiration threshold between times when the firewall or Panorama deletes logs. When a log quota reaches the maximum size, new log entries start overwriting the oldest log entries. If you reduce a log quota size, the firewall or Panorama removes the oldest logs when you commit the changes. In 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. <ul style="list-style-type: none"> Core Files—If your firewall experiences a system process failure it will generate a core file that contains details about the process and why it failed. Core files are stored in the /var/cores partition. Restore Defaults—Click to revert to the default values.
Log Card Storage and Management Card Storage tabs (Panorama template only)	If you use a Panorama template to configure log quotas and expiration periods, configure the settings in one or both of these tabs based on the firewalls assigned to the template. <p>For PA-7000 Series firewalls, logs are stored in the Log Processing Card (LPC) and Switch Management Card (SMC) and log quotas are divided 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).</p>

Item	Description
Log Export and Reporting tab	<p>Specify the following for Log Export and Reporting:</p> <ul style="list-style-type: none"> • Number of Versions for Config Audit—Enter the number of configuration versions to save before discarding the oldest ones (default is 100). You can use these saved versions to audit and compare changes in configuration. • Number of Versions for Config Backups—(Panorama only) Enter the number of configuration backups to save before discarding the oldest ones (default is 100). • Max Rows in CSV Export—Enter the maximum number of rows that will appear in the CSV reports generated when you Export to CSV from the traffic logs view (range is 1–1,048,576; default is 65,535). • Max Rows in User Activity Report—Enter the maximum number of rows that is supported for the detailed user activity reports (range is 1–1,048,576; default is 5,000). • Average Browse Time (sec)—Configure this variable to adjust how the browse time is calculated in seconds for the Monitor > PDF Reports > User Activity Report (range is 0–300 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. For 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 are assumed to be the user clicking a link within the page. The page load threshold is also used in the calculations for the Monitor > PDF Reports > User Activity Report. • Syslog HOSTNAME Format—Select whether to use the FQDN, hostname, 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 this option 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 firewall or Panorama deletes expired reports nightly at 2 a.m. according to its system time.

Item	Description
Log Export and Reporting tab (cont.)	<p>Enable Log on High DP Load—(Firewall only) Select this option if you would like a system log entry generated when the packet processing load on the firewall is at 100% CPU utilization.</p> <p>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.</p> <p>Disabled by default.</p>
Log Export and Reporting tab (Panorama only)	<p>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.</p> <p>Enabled by default.</p> <p>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 <i>primary</i> Panorama is mounted to the NFS. Therefore, the firewalls send logs to the <i>active primary</i> Panorama only.</p> <p>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).</p> <p>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.</p> <p>Only Active Primary Logs to Local Disk—Allows you to configure only the active primary Panorama to save logs to the local disk.</p> <p>This option is valid for a Panorama virtual machine with a virtual disk and to the M-Series appliance in Panorama mode.</p>
Pre-Defined Reports	<p>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.</p> <p>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 this option for the report.</p> <p>Click Select All or Deselect All to entirely enable or disable the generation of pre-defined reports.</p> <p> Before disabling a report, make sure no Group Report or a PDF Report uses it. If you disable a pre-defined report assigned to a set of reports, the entire set of reports will have no data.</p>

Item	Description
Banners and Messages	
To view all messages in a Message of the Day dialog, see Message of the Day .	
 After you configure the Message of the Day and click OK , administrators who subsequently log in and active administrators who refresh their browsers will see the new or updated message immediately; a commit isn't necessary. This enables you to warn other administrators of an impending commit before you perform that commit.	
Message of the Day (check box)	Select this option to enable the Message of the Day dialog to display upon login to the web interface.
Message of the Day (text-entry field)	Enter the text (up to 3,200 characters) for the Message of the Day dialog.
Allow Do Not Display Again	Select this option to include a Do not show again option in the Message of the Day dialog (disabled by default). This gives administrators the option to avoid seeing the message in subsequent logins.  If you modify the Message of the Day text, the message displays even to administrators who selected Do not show again . Administrators must reselect this option to avoid seeing the message in subsequent sessions.
Title	Enter text for the Message of the Day header (default is Message of the Day).
Background Color	Select a background color for the Message of the Day dialog. The default (None) is a light gray background.
Icon	Select a predefined icon to appear above the text in the Message of the Day dialog: <ul style="list-style-type: none">• None (default)• Error • Help • Information • Warning 
Header Banner	Enter the text that the header banner displays (up to 3,200 characters).
Header Color	Select a color for the header background. The default (None) is a transparent background.
Header Text Color	Select a color for the header text. The default (None) is black.
Same banner for header and footer	Select this option (enabled by default) if you want the footer banner to have the same text and colors as the header banner. When enabled, the fields for the footer banner text and colors are grayed out.
Footer Banner	Enter the text that the footer banner displays (up to 3,200 characters).
Footer Color	Select a color for the footer background. The default (None) is a transparent background.
Footer Text Color	Select a color for the footer text. The default (None) is black.

Item	Description
Minimum Password Complexity	
Enabled	<p>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.</p> <p>You can also create a password profile with a subset of these options that will override these settings and can be applied to specific accounts. For more information, see Device > Password Profiles and see Username and Password Requirements for information on valid characters that can be used for accounts.</p> <p>The maximum password length is 31 characters. Avoid setting requirements that PAN-OS does not accept. For example, do not set a requirement of 10 uppercase, 10 lower case, 10 numbers, and 10 special characters because that would exceed the maximum length of 31.</p> <p> If you have High Availability (HA) configured, always use the primary peer when configuring password complexity options and commit soon after making changes.</p> <p> Minimum password complexity settings do not apply to local database accounts for which you specified a Password Hash (see Device > Local User Database > Users).</p>
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	<p>Specify the number of sequential duplicate characters permitted in a password (range is 2-15).</p> <p>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.</p> <p>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.</p>
Block Username Inclusion (including reversed)	Select this option to prevent the account username (or reversed version of the name) from being used in the password.
New Password Differs By Characters	When administrators change their passwords, the characters must differ by the specified value.
Require Password Change on First Login	Select this option to prompt the administrators to change their passwords the first time they log in to the firewall.
Prevent Password Reuse Limit	Require that a previous password is not reused based on the specified count. Example, if the value is set to 4, you could not reuse the any of your last 4 passwords (range is 0-50).
Block Password Change Period (days)	User cannot change their passwords until the specified number of days has been reached (range is 0-365 days).

Item	Description
Required Password Change Period (days)	Require that administrators change their password on a regular basis specified 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 is 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 is 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 is 0-30 days).
AutoFocus	
Enabled	<p>Enable the firewall to connect to an AutoFocus portal to retrieve threat intelligence data and to enable integrated searches between the firewall and AutoFocus.</p> <p>When connected to AutoFocus, the firewall displays AutoFocus data associated with Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering log entries (Monitor > Logs). You can click on an artifact in these types of log entries (such as an IP address or a URL) to display a summary of the AutoFocus findings and statistics for that artifact. You can then open an expanded AutoFocus search for the artifact directly from the firewall.</p>  Check that your AutoFocus license is active on the firewall (Device > Licenses). If the AutoFocus license is not displayed, use one of the License Management options to activate the license.
AutoFocus URL	Enter the AutoFocus URL: <code>https://autofocus.paloaltonetworks.com:10443</code>
Query Timeout (sec)	Set the duration of time for the firewall to attempt to query AutoFocus for threat intelligence data. If the AutoFocus portal does not respond before the end of the specified period, the firewall will close the connection.

Device > Setup > Operations

- ▲ Device > Setup > Operations
- ▲ Panorama > Setup > Operations

You can perform the following tasks to manage the running and candidate configurations of the firewall and Panorama. If you’re using a Panorama virtual appliance, you can also use the settings on this page to configure [Log Storage Partitions for a Panorama Virtual Appliance](#).

- ▲ Manage Running and Candidate Configurations
- ▲ Enable SNMP Monitoring

Manage Running and Candidate Configurations



You must [Commit Changes](#) you make in the candidate configuration to activate those changes, at which point they become part of the running configuration. As a best practice, periodically [Save Candidate Configurations](#).

You can use [Secure Copy \(SCP\) commands from the CLI](#) to export configuration files, logs, reports, and other files to an SCP server and import the files to another firewall or Panorama. 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).

Function	Description
Configuration Management	
Revert to last saved config	Restores the default snapshot (.snapshot.xml) of the candidate configuration (the snapshot that you create or overwrite when you click Save at the top right of the web interface).
Revert to running config	Restores the current running configuration. This operation undoes all the changes you made to the candidate configuration since the last commit.
Save named configuration snapshot	Create a candidate configuration snapshot that does not overwrite the default snapshot (.snapshot.xml). Enter a Name for the snapshot or select an existing snapshot to overwrite.

Function	Description
Save candidate config	Creates or overwrites the default snapshot of the candidate configuration (.snapshot.xml). This is the same action as when you click Save at the top right of the web interface.
Load named configuration snapshot (Firewall only) or Load named Panorama configuration snapshot	Overwrites the current candidate configuration with one of the following: <ul style="list-style-type: none"> Custom-named candidate configuration snapshot (instead of the default snapshot). Custom-named running configuration that you imported. Current running configuration. The configuration must reside on the firewall or Panorama onto which you are loading it. Select the Name of the configuration and enter the Decryption Key , which is the master key of the firewall or Panorama (see Device > Master Key and Diagnostics). The master key is required to decrypt all the passwords and private keys within the configuration. If you are loading an imported configuration, you must enter the master key of the firewall or Panorama from which you imported. After the load operation finishes, the master key of the firewall or Panorama onto which you loaded the configuration re-encrypts the passwords and private keys.
Load configuration version (Firewall only) or Load Panorama configuration version	Overwrites the current candidate configuration with a previous version of the running configuration that is stored on the firewall or Panorama. Select the Name of the configuration and enter the Decryption Key , which is the master key of the firewall or Panorama (see Device > Master Key and Diagnostics). The master key is required to decrypt all the passwords and private keys within the configuration. After the load operation finishes, the master key re-encrypts the passwords and private keys.
Export named configuration snapshot	Exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location.
Export configuration version	Exports a Version of the running configuration as an XML file.
Export Panorama and devices config bundle (Panorama only)	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 Panorama > Device Deployment .
Export or push device config bundle (Panorama only)	Prompts you to select a firewall and perform one of the following actions on the firewall configuration stored on Panorama: <ul style="list-style-type: none"> Push & Commit the configuration to the firewall. This action cleans the firewall (removes any local configuration from it) and pushes the firewall configuration stored on Panorama. After you import a firewall configuration, use this option to clean that firewall so you can manage it using Panorama. Export the configuration to the firewall without loading it. To load the configuration, you must access the firewall CLI and run the configuration mode command load device-state. This command cleans the firewall in the same way as the Push & Commit option.  These options are available only for firewalls running PAN-OS 6.0.4 and later releases.

Function	Description
Export device state (Firewall only)	<p>Exports the firewall state information as a bundle. In addition to the running configuration, the state information includes device group and template settings pushed from Panorama. If the firewall is a GlobalProtect™ portal, the bundle also includes certificate information, a list of satellites that the portal manages, and satellite authentication information. If you replace a firewall or portal, you can restore the exported information on the replacement by importing the state bundle.</p> <p> You must manually run the firewall state export or create a scheduled XML API script to export the file to a remote server. This should be done on a regular basis because satellite certificates often change.</p> <p>To create the firewall state file from the CLI, from configuration mode run <code>save device state</code>. The file will be named <code>device_state_cfg.tgz</code> and is stored in <code>/opt/pancfg/mgmt/device-state</code>. The operational command to export the firewall state file is <code>scp export device-state</code> (you can also use <code>tftp export device-state</code>).</p> <p>For information on using the XML API, refer to the PAN-OS and Panorama XML API Usage Guide.</p>
Import named config snapshot	<p>Imports a running or candidate configuration from any network location. Click Browse and select the configuration file to be imported.</p>
Import device state (Firewall only)	<p>Imports the state information bundle that you exported from a firewall using the Export device state option. Besides the running configuration, the state information includes device group and template settings pushed from Panorama. If the firewall is a GlobalProtect portal, the bundle also includes certificate information, a list of satellites, and satellite authentication information. If you replace a firewall or portal, you can restore the information on the replacement by importing the state bundle.</p>

Function	Description
Import Device Configuration to Panorama (Panorama only)	<p>Imports a firewall configuration into Panorama. Panorama automatically creates a template to contain the network and device configurations. For each virtual system (vsys) on the firewall, Panorama automatically creates a device group to contain the policy and object configurations. The device groups will be one level below the Shared location in the hierarchy, though you can reassign them to a different parent device group after finishing the import (see Panorama > VMware Service Manager).</p> <p> 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.</p> <p>Configure the following import options:</p> <ul style="list-style-type: none"> • Device—Select the firewall from which Panorama will import the configurations. The drop-down includes only firewalls that are connected to Panorama and are not assigned to any device group or template. You can select only an entire firewall, not an individual vsys. • Template Name—Enter a name for the template that will contain the imported device and network settings. For a multi-vsys firewall, the field is blank. For other firewalls, the default value is the firewall name. You cannot use the name of an existing template. • 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 option is selected by default, which means Panorama imports objects that belong to Shared in the firewall to Shared in Panorama. Note that Panorama regards all objects as shared on a firewall without multiple virtual systems. If you clear this option, Panorama copies shared firewall objects into device groups instead of Shared. This setting has the following exceptions: <ul style="list-style-type: none"> • If a shared firewall object has the same name and value as an existing shared Panorama object, the import excludes that firewall object. • If the name or value of the shared firewall object differs from the shared Panorama object, Panorama imports the firewall object into each device group. • If a configuration imported into a template references a shared firewall object, Panorama imports that object into Shared regardless of whether you select this option. • If a shared firewall object references a configuration imported into a template, Panorama imports the object into a device group regardless of whether you select this option. • Rule Import Location—Select whether Panorama will import policies as pre-rules or post-rules. Regardless of your selection, Panorama imports default security rules (intrazone-default and interzone-default) into the post-rulebase. <p> 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.</p>

Function	Description
Device Operations	
Reboot	<p>To restart the firewall or Panorama, click Reboot Device. The firewall or Panorama 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 Device > Setup > Operations).</p>  If the web interface is not available, use the <code>request restart system</code> operational CLI command.
Shutdown	<p>To perform a graceful shutdown of the firewall or 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:</p> <ul style="list-style-type: none"> • All login sessions will be logged off. • Interfaces will be disabled. • All system processes will be stopped. • Existing sessions will be closed and logged. • System Logs will be created that will show the administrator name who initiated the shutdown. If this log entry cannot be written, a warning will appear and the system will not shutdown. • Disk drives will be cleanly unmounted and the firewall or Panorama will powered off. <p>You need to unplug the power source and plug it back in before you can power on the firewall or Panorama.</p>  If the web interface is not available, use the <code>request shutdown system</code> CLI command.
Restart Data Plane	<p>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.</p>  If the web interface is not available, use the <code>request restart dataplane</code> CLI command.

Function	Description
Miscellaneous	
Custom Logos	<p>Use this option to customize any of the following:</p> <ul style="list-style-type: none"> • Login Screen background image • Main UI (User Interface) header image • PDF Report Title Page image (Refer to Monitor > PDF Reports > Manage PDF Summary.) • PDF Report Footer image <p>Click  to upload an image file, click  to preview an image, or click  to remove a previously-uploaded image.</p> <p>To return to the default logo, remove your entry and Commit.</p> <p>For the Login Screen and Main UI options, clicking  displays the image as it will appear. If necessary, the firewall crops the image to fit. For PDF reports, the firewall automatically resizes the images to fit without cropping. In all cases, the preview displays the recommended image dimensions.</p> <p>The maximum image size for any logo is 128KB. The supported file types are png, gif, and jpg. The firewall does not support image files that are interlaced or that contain alpha channels; such files interfere with PDF report generation. You might need to contact the illustrator who created an image to remove alpha channels or make sure the graphics software you are using does not save files with the alpha channel feature.</p> <p>For information on generating PDF reports, see Monitor > PDF Reports > Manage PDF Summary.</p>
SNMP Setup	Enable SNMP Monitoring .
Statistics Service Setup	<p>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.</p> <p>You can allow the firewall to send any of the following types of information:</p> <ul style="list-style-type: none"> • Application and Threat Reports • Unknown Application Reports • URL Reports • Device traces for crashes <p>To view a sample of the content in a statistical report to be sent, click the report. The Report Sample tab opens to display the report code. To view a report, select the desired report, then click Report Sample.</p>
Storage Partition Setup (Panorama only)	Log Storage Partitions for a Panorama Virtual Appliance .

Enable SNMP Monitoring

▲ Device > Setup > Operations

Simple Network Management Protocol (SNMP) is a standard protocol for monitoring the devices on your network. Select **Operations** to configure the firewall to use the SNMP version that your SNMP manager supports (SNMPv2c or SNMPv3). For a list of the MIBs that you must load into the SNMP manager so it can

interpret the statistics it collects from the firewall, see [Supported MIBs](#). To configure the server profile that enables the firewall to communicate with the SNMP trap destinations on your network, see [Device > Server Profiles > SNMP Trap](#). The SNMP MIBs define all SNMP traps that the firewall generates. An SNMP trap identifies an event with a unique Object ID (OID) and the individual fields are defined as a variable binding (varbind) list. Click **SNMP Setup** and specify the following settings to allow SNMP GET requests from your SNMP manager.

Field	Description
Physical Location	Specify the physical location of the firewall. When a log or trap is generated, this information allows you to identify (in an SNMP manager) the firewall that generated the notification.
Contact	Enter the name or email address of the person responsible for maintaining the firewall. This setting is reported in the standard system information MIB.
Use Specific Trap Definitions	This option is selected by default, which means the firewall uses a unique OID for each SNMP trap based on the event type. If you clear this option, every trap will have the same OID.
Version	Select the SNMP version— V2c (default) or V3 . Your selection controls the remaining fields that the dialog displays.
For SNMP V2c	
SNMP Community String	Enter the community string, which identifies an SNMP <i>community</i> 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).
For SNMP V3	
Name / View	<p>You can assign a group of one or more views to the user of an SNMP manager to control which MIB objects (statistics) the user can get from the firewall. Each view is a paired OID and bitwise mask—the OID specifies a MIB and the mask (in hexadecimal format) specifies which objects are accessible within (include matching) or outside (exclude matching) that MIB.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p> 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.</p>

Field	Description
Users	<p>SNMP user accounts provide authentication, privacy, and access control when firewalls forward traps and SNMP managers get firewall statistics. For each user, click Add and configure the following settings:</p> <ul style="list-style-type: none">• Users—Specify a username to identify the SNMP user account. The username you configure on the firewall must match the username configured on the SNMP manager. The username can have up to 31 characters.• View—Assign a group of views to the user.• Auth Password—Specify the authentication password of the user. The firewall uses the password to authenticate to the SNMP manager when forwarding traps and responding to statistics requests. The firewall uses Secure Hash Algorithm (SHA-1 160) to encrypt the password. The password must be 8-256 characters and all characters are allowed.• Priv Password—Specify the privacy password of the user. The firewall uses the password and Advanced Encryption Standard (AES-128) to encrypt SNMP traps and responses to statistics requests. The password must be 8-256 characters and all characters are allowed.

Device > Setup > HSM

Select **Device > Setup > HSM** to configure a Hardware Security Module (HSM) and to view HSM status.

What do you want to know?	See:
What is the purpose of a Hardware Security Module (HSM) and where can I find detailed configuration procedures?	Secure Keys with a Hardware Security Module 
Configure:	Hardware Security Module Provider Settings
	HSM Authentication
How do I view HSM status?	Hardware Security Module Provider Configuration and Status
	Hardware Security Module Status

Hardware Security Module Provider Settings

To configure a Hardware Security Module (HSM) on the firewall, edit the Hardware Security Module Provider settings.

Hardware Security Module (HSM) Provider Setting	Description
Provider Configured	Select the HSM vendor: <ul style="list-style-type: none"> None—By default, the firewall does not connect to any HSM. SafeNet Network HSM Thales nShield Connect  The HSM server version must be compatible with the HSM client version  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 Network only)	Select this option 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.
Auto Recovery Retry (SafeNet Network only)	Specify the number of times that the firewall will try to recover its connection to an HSM before failing over to another HSM in an HSM high availability configuration (range is 0–500).
High Availability Group Name. (SafeNet Network 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.

HSM Authentication

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

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

Hardware Security Module Provider Configuration and Status

The Hardware Security Module Provider section shows the HSM configuration settings and the connectivity status of the HSM.

Hardware Security Module (HSM) Provider Status	Description
Provider Configured	Select the HSM vendor configured on the firewall: <ul style="list-style-type: none"> • None • SafeNet Network HSM • Thales nShield Connect
High Availability	(SafeNet Network only) HSM high availability is configured if checked.
High Availability Group Name.	(SafeNet Network only) The group name configured on the firewall for HSM high availability.
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	Shows green if the firewall is connected and authenticated to the HSM and shows red if the firewall is not authenticated or if network connectivity to the HSM is down. You can also Hardware Security Module Status for more details on the HSM connection.

Hardware Security Module Status

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

Hardware Security Module Status	Description
SafeNet Network	<ul style="list-style-type: none">• 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 connection. This field shows Authenticated if the HSM is displayed in this table.
Thales nShield Connect	<ul style="list-style-type: none">• Name—The Server name of the HSM.• IP address—The IP address of the HSM that was assigned on the firewall.• Module State—The current operating state of the HSM connection. This setting shows Authenticated if the firewall successfully authenticated to the HSM and shows Not Authenticated if authentication failed.

Device > Setup > Services

- ▲ [Configure Services for Global and Virtual Systems](#)
- ▲ [Global Services Settings](#)
- ▲ [IPv4 and IPv6 Support for Service Route Configuration Settings](#)
- ▲ [Destination Service Route](#)

Configure Services for Global and Virtual Systems

On a firewall where multiple virtual systems are enabled, select **Services** to display the **Global** and **Virtual Systems** tabs where you set services that the firewall or its virtual systems, respectively, use to operate efficiently. (If the firewall is a single virtual system or if multiple virtual systems are disabled, there are not two tabs, but just a **Services** menu.)

Select **Global** to set services for the whole firewall. These settings are also used as the default values for virtual systems that do not have a customized setting for a service.

- Edit **Services** to define the destination IP addresses of DNS servers, the Update Server, and the Proxy Server. Use the dedicated **NTP** tab to configure Network Time Protocol settings. See Table 12 for field descriptions of the available Services options.
- In **Service Features**, click **Service Route Configuration** to specify how the firewall will communicate with other servers/devices for services such as DNS, email, LDAP, RADIUS, syslog, and many more. There are two ways to configure global service routes:
 - The **Use Management Interface for all** option will force all firewall service communications with external servers through the management interface (MGT). If you select this option, you must configure the MGT interface to allow communications between the firewall and the servers/devices that provide services. To configure the MGT interface, select **Device > Setup > Management** and edit the [Management Interface Settings](#).
 - The **Customize** option allows you granular control over service communication by configuring a specific source interface and IP address that the service will use as the destination interface and destination IP address in its response. (For example, you could configure a specific source IP/interface for all email communication between the firewall and an email server, and use a different source IP/interface for Palo Alto 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 13, which indicates whether a service can be configured for the **Global** firewall or **Virtual Systems**, and whether the service supports an IPv4 and/or IPv6 source address.

The **Destination** tab is another Global service route feature that you can customize. This tab appears in the Service Route Configuration window and is described in [Destination Service Route](#).

Use the **Virtual Systems** tab to specify service routes for a single virtual system. Select a Location (virtual system) and click **Service Route Configuration**. Select **Inherit Global Service Route Configuration** or **Customize service routes for a virtual system**. If you choose to customize settings, select **IPv4** or **IPv6**. Select the one or more services you want to customize to have the same settings and click **Set Selected Service Routes**. See Table 13 for services that can be customized.

Global Services Settings

To control and redirect DNS queries between shared and specific virtual systems, you can use a [DNS proxy](#) and a [DNS Server profile](#).

Global Services Setting	Description
Services	
DNS	<p>Choose the type of DNS service—Server or DNS Proxy Object. This setting is used for all DNS queries that the firewall initiated in support of FQDN address objects, logging, and firewall management. Options include:</p> <ul style="list-style-type: none"> 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.
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 firewall 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.

Global Services Setting	Description
Authentication Type	<p>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:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

IPv4 and IPv6 Support for Service Route Configuration Settings

The following table shows IPv4 and IPv6 support for service route configurations on global and virtual systems.

Service Route Configuration Setting	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.	✓	✓	—	—

Service Route Configuration Setting	Global		Virtual System	
	IPv4	IPv6	IPv4	IPv6
Proxy—Server that is acting as Proxy to the firewall.	✓	✓	—	—
RADIUS—Remote Authentication Dial-in User Service server.	✓	✓	✓	✓
SCEP—Simple Certificate Enrollment Protocol for requesting and distributing client certificates.	✓	✓	—	—
SNMP Trap—Simple Network Management Protocol trap server.	✓	—	✓	—
Syslog—Server for system message logging.	✓	✓	✓	✓
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 (**Device > Setup > Services**), 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 13). 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.

The following table describes the destination service route settings.

Destination Service Route Setting	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.

Device > Setup > Content-ID

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

Content-ID Setting	Description
URL Filtering	
Dynamic URL Cache Timeout	Click Edit and enter the timeout (in hours). This value is used in dynamic URL filtering to determine the length of time an entry remains in the cache after it is returned from the URL filtering service. This option is applicable to URL filtering using the BrightCloud database only. For more on URL filtering, select Objects > Security Profiles > URL Filtering .
URL Continue Timeout	Specify the interval in minutes following a user's continue action before the user must press continue again for URLs in the same category (range is 1–86,400; default is 15).
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 1–86,400; 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 1–86,400; default is 1,800).
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	<p>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, select Objects > Security Profiles > URL Filtering):</p> <ul style="list-style-type: none"> • Location—Select the virtual system from the drop-down (multi-vsyst 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 Device > Certificate Management > SSL/TLS Service Profile. • Mode—Determines whether the block page is delivered transparently (it appears to originate at the blocked website) or redirects the user to the specified server. If you choose Redirect, enter the IP address for redirection. <p>Click Delete to remove an entry.</p>

Content-ID Setting	Description
Content-ID Settings	
Allow Forwarding of Decrypted Content	<p>Select this option to allow 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.</p> <p>For a firewall with multiple virtual system capability, this option is enabled for each virtual system. To enable this setting for each virtual system, go to Device > Virtual Systems.</p>
Extended Packet Capture Length	<p>Set the number of packets to capture when the extended-capture option is enabled in anti-spyware and vulnerability protection profiles (range is 1-50; default is 5).</p>
Forward datagrams exceeding UDP content inspection queue	<p>Select this option to enable forwarding of UDP datagrams and skip content inspection when the UDP content inspection queue is full. The firewall can queue up to 64 datagrams while waiting a response from the content engine. When the firewall forwards a datagram and skips content inspection due to a UDP content inspection queue overflow, it increments the <code>ctd_exceed_queue_limit</code> global counter.</p> <p>Disable this option to prevent the firewall from forwarding datagrams and skipping content inspection when the UDP content inspection queue is full. With this option disabled, the firewall drops any datagrams that exceed the queue limit and increments the <code>ctd_exceed_queue_limit_drop</code> global counter.</p> <p>This pair of global counters applies to both TCP and UDP packets.</p> <p> This option is enabled by default. Palo Alto Networks recommends that you disable this option for maximum security. Enabling this option should not result in performance degradation. Some applications may incur loss of functionality in high-volume traffic situations.</p>
Forward segments exceeding TCP App-ID inspection queue	<p>Select this option to forward segments and classify the application as <code>unknown-tcp</code> when the App-ID queue exceeds the 64-segment limit. Use the <code>appid_exceed_queue_limit</code> global counter to view the number of segments in excess of this queue regardless of whether you enabled or disabled this option.</p> <p>Disable this option to prevent the firewall from forwarding TCP segments and skipping App-ID inspection when the App-ID inspection queue is full.</p> <p> This option is enabled by default. Palo Alto Networks recommends that you disable this option for maximum security. Disabling this option may result in increased latency on streams where more than 64 segments were queued awaiting App-ID processing.</p>

Content-ID Setting	Description
Forward segments exceeding TCP content inspection queue	<p>Select this option to enable forwarding of TCP segments and skip content inspection when the TCP content inspection queue is full. The firewall can queue up to 64 segments while waiting for the content engine. When the firewall forwards a segment and skips content inspection due to a full content inspection queue, it increments the <code>ctd_exceed_queue_limit</code> global counter.</p> <p>Disable this option to prevent the firewall from forwarding TCP segments and skipping content inspection when the content inspection queue is full. With this option disabled, the firewall drops any segments that exceed the queue limit and increments the <code>ctd_exceed_queue_limit_drop</code> global counter.</p> <p>This pair of global counters applies to both TCP and UDP packets.</p> <p> This option is enabled by default. Palo Alto Networks recommends that you disable this option for maximum security. Disabling this option may result in increased latency on streams where more than 64 segments were queued awaiting content processing.</p>
Allow HTTP Header Range Option	<p>Select this option to enable the HTTP Range option. The HTTP Range option allows a client to fetch only part of a file. When a next-generation firewall in the path of a transfer identifies and drops a malicious file, it terminates the TCP session with an RST packet. If the web browser implements the HTTP Range option, it can start a new session to fetch only the remaining part of the file. This prevents the firewall from triggering the same signature again due to the lack of context into the initial session, while at the same time allowing the web browser to reassemble the file and deliver the malicious content. To prevent this, make sure this option is disabled.</p> <p>By default, the firewall allows the HTTP Range option. Palo Alto Networks recommends that you disable this option to block the HTTP Range option. Disabling this option should not impact device performance; however, HTTP file transfer interruption recovery may be impaired.</p>
X-Forwarded-For Headers	
Use X-Forwarded-For Header in User-ID	<p>Select this option to specify that User-ID reads IP addresses from the X-Forwarded-For (XFF) header in client requests for web services when the firewall is deployed between the Internet and a proxy server that would otherwise hide client IP addresses. User-ID matches the IP addresses it reads with usernames that your policies reference so that those policies can control and log access for the associated users and groups. If the header has multiple IP addresses, User-ID uses the first entry from the left.</p> <p>In some cases, the header value is a character string instead of an IP address. If the string matches a username that User-ID has mapped to an IP address, the firewall uses that username for group mapping references in policies. If no IP address mapping exists for the string, the firewall invokes the policy rules in which the source user is set to any or unknown.</p> <p>URL logs display the matched usernames in the Source User field. If User-ID cannot perform the matching or is not enabled for the zone associated with the IP address, the Source User field displays the XFF IP address with the prefix <code>x-fwd-for</code>.</p>

Content-ID Setting	Description
Strip-X-Forwarded-For Header	<p>Select this option to remove the X-Forwarded-For (XFF) header, which contains the IP address of a client requesting a web service when the firewall is deployed between the Internet and a proxy server. The firewall zeroes out the header value before forwarding the request—the forwarded packets don't contain internal source IP information.</p>  <p>Selecting this option doesn't disable the use of XFF headers for user attribution in policies; the firewall zeroes out the XFF value only after using it for user attribution.</p>
Content-ID Features	
Manage Data Protection	<p>Add additional protection for access to logs that may contain sensitive information, such as credit card numbers or social security numbers.</p> <p>Click Manage Data Protection and configure the following:</p> <ul style="list-style-type: none"> • 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	<p>Use these settings to specify the types of URLs that the firewall will track or log based on content type, such as application/pdf, application/soap+xml, application/xhtml+, text/html, text/plain, and text/xml. Container pages are set per virtual system, which you select from the Location drop-down. If a virtual system does not have an explicit container page defined, the default content types are used.</p> <p>Click Add and enter or select a content type.</p> <p>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.</p>

Device > Setup > WildFire

Select **Device > Setup > WildFire** to configure WildFire settings on the firewall and Panorama. You can enable both the WildFire cloud and a WildFire appliance to be used to perform file analysis. You can also set file size limits and session information that will be reported. After populating WildFire settings, you can specify what files to forward to the WildFire cloud or the WildFire appliance by creating a **WildFire Analysis** profile (**Objects > Security Profiles > WildFire Analysis**).



To forward decrypted content to WildFire, you need to select **Allow Forwarding of Decrypted Content** in **Device > Setup > Content-ID > URL Filtering** Settings.

WildFire Setting	Description
General Settings	
WildFire Public Cloud	<p>Enter <code>wildfire.paloaltonetworks.com</code> to use the WildFire cloud hosted in the United States to analyze files.</p> <p>To use the WildFire cloud hosted in Japan, enter <code>wildfire.paloaltonetworks.jp</code>. 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.</p>
WildFire Private Cloud	<p>Specify the IP address or FQDN of the WildFire appliance.</p> <p>The firewall sends files for analysis to the specified WildFire appliance. Panorama collects threat IDs from the WildFire appliance to enable the addition of threat exceptions in Anti-Spyware profiles (for DNS signatures only) and Antivirus profiles that you configure in device groups. Panorama also collects information from the WildFire appliance to populate fields that are missing in the WildFire Submissions logs received from firewalls running software versions earlier than PAN-OS 7.0.</p>
File Size Limits	<p>Specify the maximum file size that will be forwarded to the WildFire server. Available ranges are:</p> <ul style="list-style-type: none"> • pe (Portable Executable)—Range is 1–10MB; default 10MB • apk (Android Application)—Range is 1–50MB; default 10MB • pdf (Portable Document Format)—Range is 100KB–1,000KB; default 500KB • ms-office (Microsoft Office)—Range is 200KB–10,000KB; default 500KB • jar (Packaged Java class file)—Range is 1–10MB; default 1MB • flash (Adobe Flash)—Range is 1–10MB; default is 5MB • MacOSX (DMG/MAC-APP/MACH-O PKG files)—Range is 1–50MB; default 1MB • archive (RAR/7z archive files)—Range is 1–50MB; default 10MB <p> The preceding values might differ based on the current version of PAN-OS or the content release. To see the valid ranges, click in the Size Limit field; a pop-up displays the available range and default value.</p>

WildFire Setting	Description
Report Benign Files	<p>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.</p> <p>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.</p>
Report Grayware Files	<p>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.</p> <p> 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.</p>
Session Information Settings	
Settings	<p>Specify the information to be forwarded to the WildFire server. By default, all are selected:</p> <ul style="list-style-type: none"> • Source IP—Source IP address that sent the suspected file. • Source Port—Source port that sent the suspected file. • Destination IP—Destination IP address for the suspected file. • Destination Port—Destination port for the suspected file. • Vsys—Firewall virtual system that identified the possible malware. • Application—User application that was used to transmit the file. • User—Targeted user. • URL—URL associated with the suspected file. • Filename—Name of the file that was sent. • Email sender—Provides the sender name in WildFire logs and WildFire detailed reports when a malicious email link is detected in SMTP and POP3 traffic. • Email recipient—Provides the recipient name in WildFire logs and WildFire detailed reports when a malicious email link is detected in SMTP and POP3 traffic. • Email subject—Provides the email subject in WildFire logs and WildFire detailed reports when a malicious email link is detected in SMTP and POP3 traffic.

Device > Setup > Session

Select **Device > Setup > Session** to configure session age-out times, decryption certificate settings, and global session-related settings such as firewalling IPv6 traffic and rematching security policy to existing sessions when the policy changes. The tab has the following sections:

- [Session Settings](#)
- [Session Timeouts](#)
- [TCP Settings](#)
- [Decryption Settings: Certificate Revocation Checking](#)
- [Decryption Settings: Forward Proxy Server Certificate Settings](#)
- [VPN Session Settings](#)

Session Settings

The following table describes session settings.

Session Setting	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 is 10–65,535 packets; default 100).
ICMPv6 Error Packet Rate	Enter the average number of ICMPv6 error packets per second allowed globally through the firewall (range is 10–65,535 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 IPv6 Firewalling . All IPv6-based configurations are ignored if IPv6 is not enabled. Even if IPv6 is enabled for an interface, the IPv6 Firewalling option must also be enabled for IPv6 to function.

Session Setting	Description
Enable Jumbo Frame Global MTU	<p>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.</p> <ul style="list-style-type: none"> If you do not check Enable Jumbo Frame, the Global MTU defaults to 1500 bytes (range is 576–1,500). If you check Enable Jumbo Frame, the Global MTU defaults to 9,192 bytes (range is 9,192–9,216 bytes). <p>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.</p>
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.
NAT Oversubscription Rate	<p>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.</p> <ul style="list-style-type: none"> 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 1–65,535).
Accelerated Aging	<p>Enables accelerated aging-out of idle sessions. Select this option to enable accelerated aging and specify the threshold (%) and scaling factor.</p> <p>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.</p> <p>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.</p>

Session Setting	Description
Multicast Route Setup Buffering	Select this option to enable multicast route setup buffering, which allows the firewall to preserve the first packet in a multicast session when the multicast route or forwarding information base (FIB) entry does not yet exist for the corresponding multicast group. By default, the firewall does not buffer the first multicast packet in a new session; instead, it uses the first packet to set up the multicast route. This is expected behavior for multicast traffic. You only need to enable multicast route setup buffering if your content servers are directly connected to the firewall and your custom application cannot withstand the first packet in the session being dropped. This option is disabled by default.
Multicast Route Setup Buffer Size	If you enable Multicast Route Setup Buffering, you can tune the buffer size, which specifies the buffer size per flow (range is 1–2,000; default is 1,000.) The firewall can buffer a maximum of 5,000 packets.

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.

Session Timeouts Setting	Description
Default	Maximum length of time, in seconds, that a non-TCP/UDP or non-ICMP session can be open without a response (range is 1–15,999,999; default is 30).
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 (range is 1–15,999,999; default is 60).
• Discard TCP	Applies to TCP traffic (range is 1–15,999,999; default is 90).
• Discard UDP	Applies to UDP traffic (range is 1–15,999,999; default is 60).
ICMP	Maximum length of time that an ICMP session can be open without an ICMP response (range is 1–15,999,999; default is 6).

Session Timeouts Setting	Description
Scan	Maximum length of time, in seconds, 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 (range is 5–30; default is 10).
TCP	Maximum length of time that a TCP session remains open without a response, after a TCP session is in the Established state (after the handshake is complete and/or data transmission has started); (range is 1–15,999,999; default is 3,600).
TCP handshake	Maximum length of time, in seconds, between receiving the SYN-ACK and the subsequent ACK to fully establish the session (ranges is 1–60; default is 10).
TCP init	Maximum length of time, in seconds, between receiving the SYN and SYN-ACK before starting the TCP handshake timer (ranges is 1–60; default is 5).
TCP Half Closed	Maximum length of time, in seconds, between receiving the first FIN and receiving the second FIN or a RST (range is 1–604,800; default is 120).
TCP Time Wait	Maximum length of time, in seconds, after receiving the second FIN or a RST (range is 1–600; default is 15).
Unverified RST	Maximum length of time, in seconds, after receiving a RST that cannot be verified (the RST is within the TCP window but has an unexpected sequence number, or the RST is from an asymmetric path); (ranges is 1–600; default is 30).
UDP	Maximum length of time, in seconds, that a UDP session remains open without a UDP response (range is 1–1,599,999; default is 30).
Captive Portal	<p>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.</p> <p>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 Device > User Identification > Captive Portal Settings.</p>

TCP Settings

The following table describes TCP settings.

TCP Setting	Description
Urgent Data Flag	<p>Use this option to configure whether the firewall allows the urgent pointer (URG bit flag) in the TCP header. The urgent pointer in the TCP header is used to promote a packet for immediate processing—the firewall removes it from the processing queue and expedites it through the TCP/IP stack on the host. This process is called out-of-band processing.</p> <p>Because the implementation of the urgent pointer varies by host, select Clear to eliminate any ambiguity, by disallowing out-of-band processing so that the out-of-band byte in the payload becomes part of the payload and the packet is not processed urgently. Additionally, setting this option to Clear ensures that the firewall sees the exact stream in the protocol stack as the host for whom the packet is destined. To see a count of the number of segments in which the firewall cleared the URG flag due to setting this option to Clear, from the CLI run the <code>show counter global tcp_clear_urg</code> command.</p> <p>By default, this flag is set to Do Not Modify, which means the firewall allows packets with the URG bit flag in the TCP header and enables out-of-band processing. However, Palo Alto Networks recommends setting this option to Clear for the most secure deployment. Setting this option to Clear should not result in performance degradation; in the rare instance that applications, such as telnet, are using the urgent data feature, TCP may be impacted.</p>
Drop segments with null timestamp option	<p>The TCP timestamp records when the segment was sent and allows the firewall to verify that the timestamp is valid for that session, preventing TCP sequence number wrapping. The TCP timestamp is also used to calculate round trip time. Select this option if you want the firewall to drop packets with null timestamps. To see a count of the number of segments that the firewall dropped as a result of enabling this option, from the CLI run the <code>show counter global tcp_invalid_ts_option</code> command.</p> <p>This option is disabled by default. However, Palo Alto Networks recommends enabling it for the most secure deployment. Enabling this option should not result in performance degradation. However, if a network stack incorrectly generates segments with null TCP timestamp option value, enabling this option may result in connectivity issues.</p>
Drop segments without flag	<p>Illegal TCP segments without any flags set can be used to evade content inspection. Enable this option to configure the firewall to drop packets that have no flags set in the TCP header. To see a count of the number of segments that the firewall dropped as a result of enabling this option, from the CLI run the <code>show counter global tcp_flag_zero</code> command.</p> <p>This option is disabled by default. However, Palo Alto Networks recommends enabling this option for the most secure deployment. Enabling this option should not result in performance degradation. However, if a network stack incorrectly generates segments with no TCP flags, enabling this option may result in connectivity issues.</p>

TCP Setting	Description
Forward segments exceeding TCP out-of-order queue	Select this option if you want the firewall to forward segments that exceed the TCP out-of-order queue limit of 64 per session. If you disable this option, the firewall drops segments that exceed the out-of-order queue limit. To see a count of the number of segments that the firewall dropped as a result of enabling this option, from the CLI run the <code>show counter global tcp_exceed_flow_seg_limit</code> command. This option is enabled by default. However, Palo Alto Networks recommends disabling this option for the most secure deployment. Disabling this option may result in increased latency for the specific stream that received over 64 segments out of order. No loss of connectivity should be seen as the TCP stack should handle missing segments retransmission.

Decryption Settings: Certificate Revocation Checking

Select **Session**, and in Decryption Settings, select **Certificate Revocation Checking** to set the parameters described in the following table.

Session Features: Certificate Revocation Checking Setting	Description
Enable: CRL	Select this option to use the certificate revocation list (CRL) method to verify the revocation status of certificates. If you also enable Online Certificate Status Protocol (OCSP), the firewall first tries OCSP; if the OCSP server is unavailable, the firewall then tries the CRL method. For more information on decryption certificates, see Keys and Certificates for Decryption .
Receive Timeout: CRL	If you enabled the CRL method for verifying certificate revocation status, specify the interval in seconds (1-60; default is 5) after which the firewall stops waiting for a response from the CRL service.
Enable: OCSP	Select this option to use OCSP to verify the revocation status of certificates.
Receive Timeout: OCSP	If you enabled the OCSP method for verifying certificate revocation status, specify the interval in seconds (1-60; default is 5) after which the firewall stops waiting for a response from the OCSP responder.
Block Session With Unknown Certificate Status	Select this option to block SSL/TLS sessions when the OCSP or CRL service returns a certificate revocation status of unknown. Otherwise, the firewall proceeds with the session.
Block Session On Certificate Status Check Timeout	Select this option to block SSL/TLS sessions after the firewall registers a CRL or OCSP request timeout. Otherwise, the firewall proceeds with the session.

Session Features: Certificate Revocation Checking Setting	Description
Certificate Status Timeout	<p>Specify the interval in seconds (1-60; default is 5) after which the firewall stops waiting for a response from any certificate status service and applies any session blocking logic you optionally define. The Certificate Status Timeout relates to the OCSP/CRL Receive Timeout as follows:</p> <ul style="list-style-type: none"> • 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.

Session Features: Forward Proxy Server Certificate Setting	Description
Defined by destination host	<p>Select this option if you want PAN-OS to generate certificates based on the key that the destination server uses:</p> <ul style="list-style-type: none"> • 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. <p>This is the default setting.</p>
1024-bit RSA	<p>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.</p>
2048-bit RSA	<p>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.</p>

VPN Session Settings

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

VPN Session Setting	Description
Cookie Activation Threshold	Specify a maximum number of IKEv2 half-open IKE SAs allowed per firewall, above which cookie validation is triggered. When the number of half-open IKE SAs exceeds the Cookie Activation Threshold, the Responder will request a cookie, and the Initiator must respond with an IKE_SA_INIT containing a cookie. If the cookie validation is successful, another SA session can be initiated. A value of 0 means that cookie validation is always on. The Cookie Activation Threshold is a global firewall setting and should be lower than the Maximum Half Opened SA setting, which is also global. Range is 0-65535; default is 500.
Maximum Half Opened SA	Specify the maximum number of IKEv2 half-open IKE SAs that Initiators can send to the firewall without getting a response. Once the maximum is reached, the firewall will not respond to new IKE_SA_INIT packets (range is 1-65535; default is 65535).
Maximum Cached Certificates	Specify the maximum number of peer certificate authority (CA) certificates retrieved via HTTP that the firewall can cache. This value is used only by the IKEv2 Hash and URL feature (range is 1-4000; default is 500).

Device > High Availability

▲ 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.
- [HA Lite](#)
 - [Important Considerations for Configuring HA](#)
 - [Configure HA Settings](#)



In an HA pair, both peers must be of the same model, must be running the same PAN-OS and Content Release version, and must have the same set of licenses.

In addition, for the VM-Series firewalls, both peers must be on the same hypervisor and must have the same number of CPU cores allocated on each peer.

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.

Important Considerations for 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 Release versions should be the same on each firewall. A mismatch can prevent peer firewalls from synchronizing.
- The LEDs are green on the HA ports for the active firewall and amber on the passive firewall.
- To compare the configuration of the local and peer firewalls, using the **Config Audit** tool on the **Device** tab by selecting the desired local configuration in the left selection box and the peer configuration in the right selection box.

- Synchronize the firewalls from the web interface by clicking **Push Configuration** in the HA widget on the **Dashboard**. Note that the configuration on the firewall from which you push the configuration overwrites the configuration on the peer firewall. To synchronize the firewalls from the CLI on the active firewall, use the command `request high-availability sync-to-remote running-config`.



In a High Availability (HA) active/passive configuration with firewalls that use 10 gigabit SFP+ ports, when a failover occurs and the active firewall changes to a passive state, the 10 gigabit Ethernet port is taken down and then brought back up to refresh the port, but does not enable transmit until the firewall becomes active again. If you have monitoring software on the neighboring device, it will see the port as flapping because it is going down and then up again. This is different behavior than the action with other ports, such as the 1 gigabit Ethernet port, which is disabled and still allows transmit, so flapping is not detected by the neighboring device.

Configure HA Settings

To configure HA settings, select **Device > High Availability** and then, for each group of settings, specify the corresponding information described in the following table.

HA Setting	Description
General Tab	
Setup	<p>Specify the following settings:</p> <ul style="list-style-type: none"> 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 which peer will be active-primary (set Device ID to 0) and which will be active-secondary (set the Device ID to 1). Enable Config Sync—Select this option to enable synchronization of configuration settings between the peers. 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.

HA Setting	Description
Active/Passive Settings	<ul style="list-style-type: none">• 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.<ul style="list-style-type: none">- 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 before becoming passive. This timer is used when there are missed heartbeats or hello messages due to a link or path monitoring failure.

HA Setting	Description
Election Settings	<p>Specify or enable the following settings:</p> <ul style="list-style-type: none"> • Device Priority—Enter a priority value to identify the active firewall. The firewall with the lower value (higher priority) becomes the active firewall (range is 0–255) when the preemptive capability is enabled on both firewalls in the pair. • Heartbeat Backup—Uses the management ports on the HA firewalls to provide a backup path for heartbeat and hello messages. The management port IP address will be shared with the HA peer through the HA1 control link. No additional configuration is required. • 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 firewalls 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: <ul style="list-style-type: none"> • Recommended—Use for typical failover timer settings • Aggressive—Use for faster failover timer settings. <p> 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.</p> <ul style="list-style-type: none"> • Advanced—Allows you to customize the values to suit your network requirement for each of the following timers: <ul style="list-style-type: none"> – Promotion Hold Time—Enter the time that the passive peer (in active/passive mode) or the active-secondary peer (in active/active mode) will wait before taking over as the active or active-primary peer after communications with the HA peer have been lost. This hold time 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 (range is 8,000–60,000; default is 8,000). – Heartbeat Interval—Specify how frequently the HA peers exchange heartbeat messages in the form of an ICMP ping (range is 1,000–60,000 ms; no default). The recommended value, for example, on the PA-2000 and below models is 2,000ms. – 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 is 0–16; default is 3). The value 0 means there is no maximum (an infinite number of flaps is required before the passive firewall takes over). – Preemption Hold Time—Enter the time in minutes that a passive or active-secondary peer waits before taking over as the active or active-primary peer (range is 1–60; default is 1).

HA Setting	Description
	<ul style="list-style-type: none">- 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 is 0–60,000ms; default is 0ms).- Additional Master Hold Up Time (min)—This time interval is applied to the same event as Monitor Fail Hold Up Time (range is 0–60,000ms; default is 500ms). The additional time interval is applied only to the active peer in active/passive mode and to the active-primary peer in active/active mode. This timer is recommended to avoid a failover when both peers experience the same link/path monitor failure simultaneously.

HA Setting	Description
Control Link (HA1)/Control Link (HA1 Backup)	<p>The firewalls in an HA pair use HA links to synchronize data and maintain state information. The recommended configuration for the HA control link connection is to use the dedicated HA1 link between the two firewalls 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.</p> <p>For firewalls 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. Because the management port is 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.</p> <p>On the VM-Series firewall in AWS, the management port is used as the HA1 link.</p> <p> When using a data port for the HA control link, keep in mind that because the control messages have to communicate from the dataplane to the management plane, if a failure occurs in the dataplane, peers cannot communicate HA control link information and a failover will occur. It is best to use the dedicated HA ports, or on firewalls that do not have a dedicated HA port, use the management port.</p> <p>Specify the following settings for the primary and backup HA control links:</p> <ul style="list-style-type: none"> • 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 firewall. The HA key on this firewall must also be exported from this firewall and imported on the HA peer. Configure this setting for the primary HA1 interface. Import/export keys on the Certificates page (refer to Device > Certificate Management > 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 (range is 1,000–60,000; default is 3,000). This option monitors the physical link status of the HA1 port(s).

HA Setting	Description
<p>Data Link (HA2)</p>  <p>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.</p>	<p>Specify the following settings for the primary and backup data link:</p> <ul style="list-style-type: none"> • Port—Select the HA port. Configure this setting for the primary and backup HA2 interfaces. The backup setting is optional. • IP Address—Specify the IPv4 or IPv6 address of the HA interface for the primary and backup HA2 interfaces. The backup setting is optional. • Netmask—Specify the network mask for the HA interface for the primary and backup HA2 interfaces. The backup setting is optional. • Gateway—Specify the default gateway for the HA interface for the primary and backup HA2 interfaces. The backup setting is optional. If the HA2 IP addresses of the firewalls are in the same subnet, the Gateway field should be left blank. • Enable Session Synchronization—Enable synchronization of the session information with the passive firewall, and choose a transport option. • Transport—Choose one of the following transport options: <ul style="list-style-type: none"> • Ethernet—Use when the firewalls are connected back-to-back or through a switch (Ethertype 0x7261). • IP—Use when Layer 3 transport is required (IP protocol number 99). • UDP—Use to take advantage of the fact that the checksum is calculated on the entire packet rather than just the header, as in the IP option (UDP port 29281). The benefit of using UDP mode is the presence of the UDP checksum to verify the integrity of a session sync message. • 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 option to monitor the health of the HA2 data link between HA peers. This option is disabled by default and you can enable it on one or both peers. If enabled, the peers will use keep-alive messages to monitor the HA2 connection to detect a failure based on the Threshold you set (default is 10000 ms). If you enable HA2 keep-alive, the HA2 Keep-alive recovery Action will be taken. Select an Action: <ul style="list-style-type: none"> • Log Only—Logs the failure of the HA2 interface in the system log as a critical event. Select this option for active/passive deployments because the active peer is the only firewall forwarding traffic. The passive peer is in a backup state and is not forwarding traffic; therefore a split datapath is not required. If you have not configured any HA2 Backup links, state synchronization will be turned off. If the HA2 path recovers, an informational log will be generated. • Split Datapath—Select this option in active/active HA deployments to instruct each peer to take ownership of their local state and session tables when it detects an HA2 interface failure. Without HA2 connectivity, no state and session synchronization can happen; this action allows separate management of the session tables to ensure successful traffic forwarding by each HA peer. To prevent this condition, configure an HA2 Backup link. • Threshold (ms)—The duration in which keep-alive messages have failed before one of the above actions will be triggered (range is 5,000–60,000ms; default is 10,000ms).

HA Setting	Description
Link and Path Monitoring Tab (Not available for the VM-Series firewall in AWS)	
Path Monitoring	<p>Specify the following:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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 addresses to be monitored. • Ping Interval—Specify the interval between pings that are sent to the destination address (range is 200–60,000 milliseconds; default is 200 milliseconds). • Ping Count—Specify the number of failed pings before declaring a failure (range is 3–10 pings; default is 10 pings).
Link Monitoring	<p>Specify the following:</p> <ul style="list-style-type: none"> • 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	<p>Define one or more link groups to monitor specific Ethernet links. To add a link group, specify the following and click Add:</p> <ul style="list-style-type: none"> • Name—Enter a link group name. • Enabled—Enable the link group. • Failure Condition—Select whether a failure occurs when any or all of the selected links fail. • Interfaces—Select one or more Ethernet interfaces to be monitored.
Active/Active Config Tab	
Packet Forwarding	<p>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.</p>

HA Setting	Description
HA3 Interface	<p>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.</p>  <p>If the HA3 link fails, the active-secondary peer will transition to the non-functional state. To prevent this condition, configure a Link Aggregation Group (LAG) interface with two or more physical interfaces as the HA3 link. The firewall does not support an HA3 Backup link. An aggregate interface with multiple interfaces will provide additional capacity and link redundancy to support packet forwarding between HA peers.</p>  <p>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.</p>
VR Sync	<p>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.</p>
QoS Sync	<p>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.</p>
Tentative Hold Time (sec)	<p>When a firewall in an HA active/active configuration fails, it will go into a tentative state. The transition from tentative state to active-secondary state triggers the Tentative Hold Time, during which the firewall attempts to build routing adjacencies and populate its route table before it will process any packets. Without this timer, the recovering firewall would enter the active-secondary state immediately and would blackhole packets because it would not have the necessary routes (default 60 seconds).</p>
Session Owner Selection	<p>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:</p> <ul style="list-style-type: none"> • 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 firewall receives the first packet, it will forward all packets requiring Layer 7 inspection to the active-primary firewall over the HA3 link.

HA Setting	Description
Session Setup	<p>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:</p> <ul style="list-style-type: none"> • Primary Device—The active-primary firewall sets up all sessions. • IP Modulo—Distributes session setup based on the parity of the source IP address. • IP Hash—Distributes session setup 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.
Virtual Address	<p>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.</p> <ul style="list-style-type: none"> • Floating—Enter an IP address that will move between HA peers in the event of a link or system failure. Configure two floating IP addresses on the interface, so that each firewall will own one and then set the priority. If either firewall fails, the floating IP address transitions to the HA peer. <ul style="list-style-type: none"> – Device 0 Priority—Set the priority for the firewall with Device ID 0 to determine which firewall will own the floating IP address. A firewall with the lowest value will have the highest priority. – Device 1 Priority—Set the priority for the firewall with Device ID 1 to determine which firewall will own the floating IP address. A firewall with the lowest value will have the highest priority. – Failover address if link state is down—Use the failover address when the link state is down on the interface. – Floating IP bound to the Active-Primary HA device—Select this option to bind the floating IP address to the active-primary peer. In the event one peer fails, traffic is sent continuously to the active-primary peer even after the failed firewall recovers and becomes the active-secondary peer. • 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: <ul style="list-style-type: none"> • 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.

HA Setting	Description
Operational Commands	
Suspend local device (or Make local device functional)	<p>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.</p> <p>To place a suspended firewall back into a functional state, use the following operational mode CLI command:</p> <pre>request high-availability state functional</pre> <p>To test failover, you can either uncable the active (or active-primary) firewall or you can click this link to suspend the active firewall.</p>

Device > Config Audit

Select **Device > Config Audit** to see the differences between configuration files. The page displays the configurations side by side in separate panes and highlights the differences line by line using colors to indicate additions (green), modifications (yellow), and deletions (red):

Added **Modified** **Deleted**

The following table describes the config audit settings.

Config Audit Setting	Description
Configuration name drop-downs (unlabeled)	Select two configurations to compare in the (unlabeled) configuration name drop-downs (the defaults are Running config and Candidate config).  You can filter a drop-down by entering a text string derived from the Description value of the commit operation associated with the desired configuration (see Commit Changes).
Context drop-down	Use the Context drop-down to specify the number of lines to display before and after the highlighted differences in each file. Specifying more lines can help you correlate the audit results to settings in the web interface. If you set the Context to All , the results include the entire configuration files.
Go	Click Go to start the audit.
Previous () and Next ()	These navigation arrows are enabled when consecutive configuration versions are selected in the configuration name drop-downs. Click  to compare the previous pair of configurations in the drop-downs or click  to compare the next pair of configurations.

Device > Password Profiles

- ▲ Device > Password Profiles
- ▲ Panorama > Password Profiles

Select **Device > Password Profiles** or **Panorama > Password Profiles** to set basic password requirements for individual local accounts. Password profiles override any **Minimum Password Complexity** settings you defined for all local accounts (**Device > Setup > Management**).

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



You cannot assign password profiles to administrative accounts that use local database authentication (see [Device > Local User Database > Users](#)).

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

Password Profile Setting	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 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 is 0-30).
Post Expiration Admin Login Count	Allow the administrator to log in a specified number of times after their account has expired. Example, if the value is set to 3 and their account has expired, they can log in 3 more times before their account is locked out (range is 0-3).
Post Expiration Grace Period (days)	Allow the administrator to log in the specified number of days after their account has expired (range is 0-30).

Username and Password Requirements

The following table lists the valid characters that can be used in usernames and passwords for PAN-OS and Panorama accounts.

Account Type	Username and Password Restrictions
Password Character Set	There are no restrictions on any password field character sets.
Remote Admin, SSL-VPN, or Captive Portal	<p>The following characters are not allowed for the username:</p> <ul style="list-style-type: none"> • Backtick (`) • Angular brackets (< and >) • Ampersand (&) • Asterisk (*) • At sign (@) • Question mark (?) • Pipe () • Single-Quote ('') • Semicolon (;) • Double-Quote ("") • Dollar (\$) • Parentheses ('(' and ')') • Colon (':')
Local Administrator Accounts	<p>The following are the allowed characters for local usernames:</p> <ul style="list-style-type: none"> • Lowercase (a-z) • Uppercase (A-Z) • Numeric (0-9) • Underscore (_) • Period (.) • Hyphen (-) <p> Login names cannot start with a hyphen (-).</p>

Device > Administrators

Administrator accounts control access to firewalls and Panorama. A firewall administrator can have full or read-only access to a single firewall or to a virtual system on a single firewall. Firewalls have a predefined **admin** account that has full access.



To define Panorama administrators, see [Panorama > Managed Devices](#).

The following authentication options are supported:

- **Password authentication**—The administrator enters a username and password to log in. This authentication requires no certificates. You can use it in conjunction with authentication profiles, or for local database authentication.
- **Client certificate authentication (web)**—This authentication requires no username or password; the certificate suffices to authenticate access to the firewall.
- **Public key authentication (SSH)**—The administrator generates a public/private key pair on the machine that requires access to the firewall, and then uploads the public key to the firewall to allow secure access without requiring the administrator to enter a username and password.

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

Administrator Account Setting	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 Device > Authentication Profile .
Use only client certificate authentication (web)	Select this option to use client certificate authentication for web access. If you select this option, a username and password are not required; the certificate is sufficient to authenticate access to the firewall.
New Password Confirm New Password	Enter and confirm a case-sensitive password for the administrator (up to 31 characters). You can also select Setup > Management to enforce a minimum password length.  To ensure that the firewall management interface remains secure, we recommend that you periodically change administrative passwords using a mixture of lower-case letters, upper-case letters, and numbers. You can also configure Minimum Password Complexity settings for all administrators on the firewall.

Administrator Account Setting	Description
Use Public Key Authentication (SSH)	<p>Select this option to use SSH public key authentication. Click Import Key and browse to select the public key file. The uploaded key appears in the read-only text area.</p> <p>Supported key file formats are IETF SECSH and OpenSSH. Supported key algorithms are DSA (1024 bits) and RSA (768-4096 bits).</p>  If the public key authentication fails, the firewall prompts the administrator for a username and password.
Role	<p>Assign a role to this administrator. The role determines what the administrator can view and modify.</p> <p>If you select Role Based, select a custom role profile from the drop-down. For details, see Device > Admin Roles.</p> <p>If you select Dynamic, you can select one of the following predefined roles:</p> <ul style="list-style-type: none"> • Superuser—Has full access to the firewall and can define new administrator accounts and virtual systems. You must have superuser privileges to create an administrative user with superuser privileges. • Superuser (read-only)—Has read-only access to the firewall. • Device administrator—Has full access to all firewall settings except for defining new accounts or virtual systems. • Device administrator (read-only)—Has read-only access to all firewall settings except password profiles (no access) and administrator accounts (only the logged in account is visible). • Virtual system administrator—Has full access to specific virtual systems on the firewall (if multiple virtual systems are enabled). • Virtual system administrator (read-only)—Has read-only access to specific virtual systems on the firewall (if multiple virtual systems are enabled).
Virtual System (Virtual system administrator role only)	<p>Click Add to select the virtual systems that the administrator can manage.</p>
Password Profile	<p>Select the password profile, if applicable. To create a new password profile, see Device > Password Profiles.</p>

Device > Admin Roles

Select **Device > Admin Roles** to define Admin Role profiles, which are custom roles that determine the access privileges and responsibilities of administrative users. You assign **Admin Role profiles or dynamic roles** when you **Device > Administrators**.



To define Admin Role profiles for Panorama administrators, see [Panorama > Managed Devices](#).

The firewall has three predefined roles you can use for common criteria purposes. You first use the superuser role for initial firewall configuration and to create the administrator accounts for the Security Administrator, Audit Administrator, and Cryptographic Administrator. After you create these accounts and apply the proper common criteria Admin Roles, you then log in using those accounts. The default superuser account in Federal Information Processing Standard (FIPS)/Common Criteria (CC) FIPS-CC mode is `admin` and 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 (such as creating the firewall security policy) not addressed by the other two administrative roles.

To add an Admin Role profile, click **Add** and specify the following information.

Administrator Role Setting	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	(Optional) Enter a description for the role (up to 255 characters).
Role	Select the scope of administrative responsibility: <ul style="list-style-type: none">• Device—The role applies to the entire firewall, regardless whether it has more than one virtual system (vsys).• Virtual System—The role applies to specific virtual systems on the firewall. You select the virtual systems when you Device > Administrators.
WebUI	Click the icons for specific web interface features to set the permitted access privileges: <ul style="list-style-type: none">• Enable—Read/write access to the selected feature.• Read Only—Read-only access to the selected feature.• Disable—No access to the selected feature.
XML API	Click the icons for specific XML API features to set the permitted access privileges (Enable , Read Only , or Disable).

Administrator Role Setting	Description
Command Line	<p>Select the type of role for CLI access. The default is None, which means access to the CLI is not permitted. The other options vary by Role scope:</p> <ul style="list-style-type: none"> • Device <ul style="list-style-type: none"> • superuser—Has full access to the firewall and can define new administrator accounts and virtual systems. You must have superuser privileges to create an administrative user with superuser privileges. • superreader—Has read-only access to the firewall. • deviceadmin—Has full access to all firewall settings except for defining new accounts or virtual systems. • devicereader—Has read-only access to all firewall settings except password profiles (no access) and administrator accounts (only the logged in account is visible). • Virtual System <ul style="list-style-type: none"> • vsysadmin—Has full access to specific virtual systems on the firewall. • vsysreader—Has read-only access to specific virtual systems on the firewall.

Device > Access Domain

- ▲ Device > Access Domain
- ▲ Panorama > Access Domain

Select **Device > Access Domain** or **Panorama > Access Domain** 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 [Device > Server Profiles > RADIUS](#)). On Panorama, you can manage access domains locally or using RADIUS VSAs (see [Panorama > Access Domains](#)).

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 firewall or Panorama. If RADIUS is not used, the access domain settings on this page are ignored.

Access Domain Setting	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 firewalls that support virtual systems.

Device > Authentication Profile

- ▲ Device > Authentication Profile
- ▲ Panorama > Authentication Profile

Select **Device > Authentication Profile** or **Panorama > Authentication Profile** to configure authentication settings that you can apply to administrator accounts, SSL-VPN access, and Captive Portal. The firewall and Panorama support local, RADIUS, TACACS+, LDAP, and Kerberos authentication services.



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.

Authentication Profile Setting	Description
Name	<p>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.</p> <p> 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.</p>
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 .

Authentication Tab

Type	<p>Select the authentication type:</p> <ul style="list-style-type: none"> • 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 Device > Server Profiles > RADIUS , Device > Server Profiles > TACACS+ , Device > Server Profiles > LDAP , and Device > Server Profiles > Kerberos .
Retrieve User Group	If the authentication Type is RADIUS , select 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.

Authentication Profile Setting	Description
Password Expiry Warning	<p>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 is 1–255). Users will not be able to access the VPN if their passwords expire.</p>  <ul style="list-style-type: none"> Consider configuring the agents to use pre-logon connect method. This will enable users to connect to the domain to change their passwords even after the password has expired. If users allow their passwords to expire, the administrator can assign a temporary LDAP password to enable users to log in to the VPN. In this workflow, we recommend setting the Authentication Modifier in the portal configuration to Cookie authentication for config refresh (otherwise, the temporary password will be used to authenticate to the portal, but the gateway login will fail, preventing VPN access).
User Domain and Username Modifier	<p>The firewall combines the User Domain and Username Modifier values to modify the domain/username string that a user enters during login. The firewall uses the modified string for authentication and uses the User Domain value for User-ID group mapping. Select from the following options:</p> <ul style="list-style-type: none"> 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%.  <p>If the Username Modifier includes the %USERDOMAIN% variable, the User Domain value replaces any domain string that the user enters. If you specify the %USERDOMAIN% variable and leave the User Domain blank, the firewall removes any user-entered domain string. The firewall resolves domain names to the appropriate NetBIOS name for User-ID group mapping. This applies to both parent and child domains. User Domain modifiers take precedence over automatically derived NetBIOS names.</p>
Kerberos Realm	<p>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.</p>

Authentication Profile Setting	Description
Kerberos Keytab	<p>If your network supports Kerberos single sign-on (SSO), click Import, click Browse to locate the keytab file, and then click OK. A keytab contains Kerberos account information (principal name and hashed password) for the firewall, which is required for SSO authentication. Each authentication profile can have one keytab. During authentication, the firewall first tries to use the keytab to establish SSO. If it succeeds and the user attempting access is in the Allow List, authentication succeeds immediately. Otherwise, the authentication process falls back to manual (username/password) authentication of the specified Type, which doesn't have to be Kerberos. For details on creating keytabs, see the PAN-OS 7.1 Administrator's Guide.</p> <p> If the firewall is in FIPS/CC mode, the algorithm must be aes128-cts-hmac-sha1-96 or aes256-cts-hmac-sha1-96. Otherwise, you can also use des3-cbc-sha1 or arcfour-hmac. 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 fails. Your Kerberos administrator determines which algorithms the service tickets use.</p>
Advanced Tab	
Allow List	<p>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.</p> <p> 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.</p> <p>To remove users or user groups, select them and click Delete.</p>
Failed Attempts	<p>Enter the number of failed login attempts (1-10) that the firewall allows before locking out the user account. A value of 0 (default) specifies unlimited login attempts. Limiting login attempts can help protect against brute force attacks.</p> <p> 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.</p>
Lockout Time	<p>Enter the number of minutes (0-60) for which the firewall 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.</p> <p> 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.</p>

Device > 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 firewall tries to use for authenticating users when they log in. The firewall tries the profiles sequentially from the top of the list to the bottom—applying the authentication, Kerberos single sign-on, allow list, and account lockout values for each—until one profile successfully authenticates the user. The firewall only denies access if all profiles in the sequence fail to authenticate. For details on authentication profiles, see [Device > Authentication Profile](#).

Authentication Sequence Setting	Description
Name	<p>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.</p> <p> 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.</p>
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 option (selected by default) if you want the firewall to match the domain name that a user enters during login with the User Domain or Kerberos Realm of an authentication profile associated with the sequence and then use that profile to authenticate the user. The user input that the firewall uses for matching can be the text preceding the username (with a backslash separator) or the text following the username (with a @ separator). If the firewall does not find a match, it tries the authentication profiles in the sequence in top-to-bottom order.
Authentication 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 .

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).



When monitoring ESXi hosts that are part of the VM-Series NSX edition solution, use Dynamic Address Groups instead of using VM Information Sources to learn about changes in the virtual environment. For the VM-Series NSX edition solution, the NSX Manager provides Panorama with information on the NSX security group to which an IP address belongs. The information from the NSX Manager provides the full context for defining the match criteria in a Dynamic Address Group because it uses the service profile ID as a distinguishing attribute and allows you to properly enforce policy when you have overlapping IP addresses across different NSX security groups.

A maximum of 32 tags (from vCenter server and NSX Manager) can be registered to an IP address.

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 information sources.

For information on how VM Information Sources and Dynamic Address Groups can work synchronously and enable you to monitor changes in the virtual environment, refer to the *VM-Series Deployment Guide*.

- For IP address to 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.



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.

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
<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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 to 5 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 [Settings to Enable VM Information Sources for VMware ESXi and vCenter Servers](#).
- For AWS-VPC, see [Settings to Enable VM Information Sources for AWS VPC](#).

Refresh Connected—Click to refresh the connection status; it refreshes the onscreen display. This option 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.

Settings to Enable VM Information Sources for VMware ESXi and vCenter Servers

The following table describes settings you can configure to enable VM information sources for VMware ESXi and vCenter servers.

Setting to Enable VM Information Sources for VMware ESXi and vCenter Servers	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).

Setting to Enable VM Information Sources for VMware ESXi and vCenter Servers	Description
Enabled	<p>By default the communication between the firewall and the configured source is enabled.</p> <p>The connection status between the monitored source and the firewall displays in the interface as follows:</p> <ul style="list-style-type: none"> ● —Connected ● —Disconnected ● —Pending (The connection status may also display as yellow when the monitored source is disabled.) <p>Clear the Enabled option to disable communication between the host and the firewall.</p>
Timeout	<p>Enter the interval in hours after which the connection to the monitored source is closed, if the host does not respond (range is 2–10; default is 2).</p> <p>(Optional) To change the default value, select this option 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.</p>
Source	Enter the FQDN or the IP address of the host/source being monitored.
Username	Specify the username required to authenticate to the source.
Password	Enter the password and confirm your entry.
Update Interval	Specify the interval, in seconds, at which the firewall retrieves information from the source (range is 5–600; default is 5).

Settings to Enable VM Information Sources for AWS VPC

The following table describes the setting you configure to enable VM information sources for an AWS VPC.

Setting to Enable VM Information Sources for an AWS VPC	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.

Setting to Enable VM Information Sources for an AWS VPC	Description
Enabled	<p>By default the communication between the firewall and the configured source is enabled.</p> <p>The connection status between the monitored source and the firewall displays in the interface as follows:</p> <ul style="list-style-type: none"> • —Connected • —Disconnected • —Pending (The connection status may also display as yellow when the monitored source is disabled.) <p>Clear the Enabled option to disable communication between the host and the firewall.</p>
Source	<p>Add the URI in which the Virtual Private Cloud resides in the following format: <code>ec2.<your_AWS_region>.amazonaws.com</code>.</p> <p>For example, <code>ec2.us-west-1.amazonaws.com</code>.</p>
Access Key ID	<p>Enter the alphanumeric text string that uniquely identifies the user who owns or is authorized to access the AWS account.</p> <p>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.</p>
Secret Access Key	Enter the password and confirm your entry.
Update Interval	Specify the interval, in seconds, at which the firewall retrieves information from the source (range is 60–1,200; default is 60).
Timeout	<p>The interval in hours after which the connection to the monitored source is closed, if the host does not respond (default is 2)</p> <p>(Optional) Select this option 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.</p>
VPC ID	<p>Enter the ID of the AWS-VPC to monitor, for example, <code>vpc-1a2b3c4d</code>. Only EC2 instances that are deployed within this VPC are monitored.</p> <p>If your account is configured to use a default VPC, the default VPC ID will be listed under AWS Account Attributes.</p>

Device > Virtual Systems

A **virtual system (vsys)**  is an independent (virtual) firewall instance that you can separately manage within a physical firewall. Each vsys can be an independent firewall with its own security policy, interfaces, and administrators; a vsys enables you to segment the administration of all policies, reporting, and visibility functions that the firewall provides. For example, if you want to customize the security features for the traffic that is associated with your Finance department, you can define a Finance vsys and then define security policies that pertain only to that department. To optimize policy administration, you can maintain separate administrator accounts for overall firewall and network functions while creating vsys administrator accounts that allow access to 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 firewall- 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, PA-5000, and PA-7000 Series firewalls support multiple virtual systems. The PA-2000 and PA-3000 Series firewalls can support multiple virtual systems only if the appropriate license is installed. The PA-200 and PA-500 firewalls do not support multiple virtual systems.

Additional points to consider before enabling multiple virtual systems:

- 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 [Device > Setup > Services](#)).

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

Virtual System Setting	Description
ID	<p>Enter an integer identifier for the vsys. Refer to the data sheet for your firewall model for information on the number of supported vsys.</p>  If you use a Panorama template to configure the vsys, this field does not appear.
Name	<p>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.</p>  If you use a Panorama template to push vsys configurations, the vsys name in the template must match the vsys name on the firewall.
Allow Forwarding of Decrypted Content	Select this option to allow the virtual system to forward decrypted content to an outside service when port mirroring or sending WildFire files for analysis. For information on Decryption Port Mirroring, see Decryption Port Mirroring .
General Tab	<p>Select a DNS Proxy object if you want to apply DNS proxy rules to this vsys. See Network > DNS Proxy.</p> <p>To include objects of a particular type, select 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.</p>
Resource Tab	<p>Specify the resource limits allowed for this virtual system. Each field displays the valid ranges; there are no default values.</p> <ul style="list-style-type: none"> • Sessions Limit—Maximum number of sessions. (If you use the <code>show session meter</code> CLI command, it displays the Maximum number of sessions allowed per dataplane, the Current number of sessions being used by the virtual system, and the Throttled number of sessions per virtual system. On a PA-7000 Series firewall, the Current number of sessions can be greater than the Maximum configured for Sessions Limit because there are multiple dataplanes per virtual system. The Sessions Limit you configure on a PA-7000 Series firewall is per dataplane, and will result in a higher maximum per virtual system.) • Security Rules—Maximum number of security rules. • NAT Rules—Maximum number of NAT rules. • Decryption Rules—Maximum number decryption rules. • 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.

Device > Shared Gateways

Shared gateways allow multiple virtual systems to share a single interface for external communication (typically connected to a common upstream network such as an Internet Service Provider). All of the virtual systems communicate with the outside world through the physical interface using a single IP address. A single virtual router is used to route traffic for all of the virtual systems through the shared gateway.

Shared gateways use Layer 3 interfaces, and at least one Layer 3 interface must be configured as a shared gateway. Communications originating in a virtual system and exiting the firewall through a shared gateway require similar policy to communications passing between two virtual systems. You could configure an 'External vsys' zone to define security rules in the virtual system.

Shared Gateway Setting	Description
ID	Identifier for the gateway (not used by firewall).
Name	Enter a name for the shared gateway (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. Only the name is required.
DNS Proxy	(Optional) If a DNS proxy is configured, select which DNS server(s) to use for domain name queries.
Interfaces	Select the interfaces the shared gateway will use.

Device > Certificate Management

- ▲ [Device > Certificate Management > Certificates](#)
- ▲ [Device > Certificate Management > Certificate Profile](#)
- ▲ [Device > Certificate Management > OCSP Responder](#)
- ▲ [Device > Certificate Management > SSL/TLS Service Profile](#)
- ▲ [Device > Certificate Management > SCEP](#)

Device > Certificate Management > Certificates

Select **Device > Certificate Management > Certificates > Device Certificates** to manage (generate, import, renew, delete, and revoke) certificates, which are used to secure communication across a network. You can also export and import the high availability (HA) key that secures the connection between HA peers on the network. Select **Device > Certificate Management > Certificates > Default Trusted Certificate Authorities** to view, enable, and disable the certificate authorities (CAs) that the firewall trusts.



For more information on how to implement certificates on the firewall and Panorama, refer to [Certificate Management](#).

- [Manage Firewall and Panorama Certificates](#)
- [Manage Default Trusted Certificate Authorities](#)

Manage Firewall and Panorama Certificates

- ▲ [Device > Certificate Management > Certificates > Device Certificates](#)
- ▲ [Panorama > Certificate Management > Certificates](#)

Select **Device > Certificate Management > Certificates > Device Certificates** or **Panorama > Certificate Management > Certificates > Device Certificates** to display the certificates that the firewall or Panorama uses for tasks such as securing access to the web interface, SSL decryption, or LVPN.

The following are some uses for certificates. Define the usage of the certificate after you generate it (see [Manage Default Trusted Certificate Authorities](#)).

- **Forward Trust**—The firewall uses this certificate to sign a copy of the server certificate that the firewall presents to clients during [SSL Forward Proxy decryption](#) when the certificate authority (CA) that signed the server certificate is in the trusted CA list on the firewall.
- **Forward Untrust**—The firewall uses this certificate to sign a copy of the server certificate the firewall presents to clients during [SSL Forward Proxy decryption](#) when the CA that signed the server certificate is not in the trusted CA list on the firewall.
- **Trusted Root CA**—The firewall uses this certificate as a trusted CA for [SSL Forward Proxy decryption](#), [GlobalProtect](#), [URL Admin Override](#), and [Captive Portal](#). The firewall has a large list of existing trusted CAs. The trusted root CA certificate is for additional CAs that your organization trusts but that are not part of the pre-installed trusted list.
- **SSL Exclude**—The firewall uses this certificate if you [configure decryption exceptions](#) to exclude specific servers from SSL/TLS decryption.
- **Certificate for Secure Syslog**—The firewall uses this certificate to secure the [delivery of logs as syslog messages](#) to a syslog server.

To generate a certificate, click Generate and specify the following fields.

Setting to Generate a Certificate	Description
Certificate Type	Select the entity that generates the certificate: <ul style="list-style-type: none"> ● Local—The firewall or Panorama generates the certificate. ● SCEP—A Simple Certificate Enrollment Protocol (SCEP) server generates the certificate and sends it to the firewall or Panorama.

Setting to Generate a Certificate	Description
Certificate Name	(Required) 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.
SCEP Profile	<p>(SCEP certificates only) Select a SCEP Profile to define how the firewall or Panorama communicates with a SCEP server and to define settings for the SCEP certificate. For details, see Device > Certificate Management > SCEP. You can configure a firewall that serves as a GlobalProtect portal to request SCEP certificates on demand and automatically deploy the certificates to endpoints.</p> <p>The remaining fields in the Generate Certificate dialog do not apply to SCEP certificates. After specifying the Certificate Name and SCEP Profile, click Generate.</p>
Common Name	(Required) Enter the IP address or FQDN that will appear on the certificate.
Shared	On a firewall that has more than one virtual system (vsys), select Shared if you want the certificate to be available to every vsys.
Signed By	<p>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.</p> <p>If you have imported CA certificates or have issued them on the firewall (self-signed), the drop-down includes the CAs available to sign the certificate that is being created.</p> <p>To generate a certificate signing request (CSR), select External Authority [CSR]. The firewall generates the certificate and the key pair and you can then export the CSR.</p>
Certificate Authority	<p>Select this option if you want the firewall to issue the certificate.</p> <p>Marking this certificate as a CA allows you to use this certificate to sign other certificates on the firewall.</p>
OCSP Responder	Select an OCSP responder profile from the drop-down (see Device > Certificate Management > OCSP Responder). The corresponding host name appears in the certificate.
Algorithm	<p>Select a key generation algorithm for the certificate—RSA or Elliptic Curve DSA (ECDSA).</p> <p> 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.</p> <p> 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.</p>
Number of Bits	<p>Select the key length for the certificate.</p> <p>If the firewall is in FIPS-CC mode and the key generation Algorithm is RSA, the RSA keys generated must be 2048 or 3027 bits. If the Algorithm is Elliptic Curve DSA, both key length options (256 and 384) work.</p>

Setting to Generate a Certificate	Description
Digest	<p>Select the Digest algorithm for the certificate. The available options depend on the key generation Algorithm:</p> <ul style="list-style-type: none"> • RSA—MD5, SHA1, SHA256, SHA384, or SHA512 • Elliptic Curve DSA—SHA256 or SHA384 <p>If the firewall is in FIPS-CC mode and the key generation Algorithm is RSA, you must select SHA256, SHA384, or SHA512 as the Digest algorithm. If the Algorithm is Elliptic Curve DSA, both Digest algorithms (SHA256 and SHA384) work.</p>  Client certificates that are used when requesting firewall services that rely on TLSv1.2 (such as administrator access to the web interface) cannot have SHA384 (in releases before PAN-OS 7.1.8) or SHA512 as a digest algorithm. The client certificates must use a lower digest algorithm or you must limit the Max Version to TLSv1.1 when you configure SSL/TLS service profiles for the firewall services (see Device > Certificate Management > SSL/TLS Service Profile).
Expiration (days)	<p>Specify the number of days that the certificate will be valid. The default is 365 days.</p>  If you specify a Validity Period in a GlobalProtect satellite configuration, that value will override the value entered in this field.
Certificate Attributes	<p>Add additional Certificate Attributes to identify the entity to which you are issuing the certificate. You can add any of the following attributes—Country, State, Locality, Organization, Department, and Email.</p> <p>You can also specify one of the following Subject Alternative Name fields—Host Name (SubjectAltName:DNS), IP (SubjectAltName:IP), and Alt Email (SubjectAltName:email).</p>  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 certificate details display on the page.

Supported Action to Manage Certificates	Description
Delete	<p>Select the certificate and click Delete.</p>  If the firewall has a decryption policy, you cannot delete a certificate for which the usage is set to Forward Trust Certificate or Forward Untrust Certificate . To change the certificate usage, see Manage Default Trusted Certificate Authorities .
Revoke	<p>Select the certificate that you want to revoke, and click Revoke. The certificate will be instantly set to revoked status. No commit is required.</p>

Supported Action to Manage Certificates	Description
Renew	<p>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.</p> <p>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.</p> <p>If an external certificate authority (CA) signed the certificate and the firewall uses the Online Certificate Status Protocol (OCSP) to verify certificate revocation status, the firewall uses the OCSP responder information to update the certificate status</p>
Import	<p>To import a certificate, click Import and configure the fields as follows:</p> <ul style="list-style-type: none"> 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 Private key resides on Hardware Security Module if an HSM stores the key for this certificate. For HSM details, see Monitor > Automated Correlation Engine. Select Import private key if you also want to import the private key. 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.
Export	<p>Select the certificate you want to export, click Export, and select a File Format:</p> <ul style="list-style-type: none"> Encrypted Private Key and Certificate (PKCS12)—The exported file will contain both the certificate and private key. Base64 Encoded Certificate (PEM)—If you want to export the private key also, select Export Private Key and enter a Passphrase and Confirm Passphrase. Binary Encoded Certificate (DER)—You can export only the certificate, not the key—ignore Export Private Key and passphrase fields.
Import HA Key	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.
Export HA Key	To import keys for high availability (HA), click Import HA Key and Browse to specify the key file for import.
Define the usage of the certificate	To export keys for HA, click Export HA Key and specify a location to save the file.
Define the usage of the certificate	In the Name column, select the certificate and then select options appropriate for how you plan to use the certificate.

Manage Default Trusted Certificate Authorities

▲ Device > Certificate Management > Certificates > Default Trusted Certificate Authorities

Use this page to view, disable, or export, the pre-included certificate authorities (CAs) that the firewall trusts. 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.

Trusted Certificate Authorities Setting	Description
Enable	If you have disabled a CA and want to re-enable it, click Enable .
Disable	Select the CA you want to disable and then click Disable . You might use this option if you want to trust only specific CAs or you want to remove all of them and trust only your local CA.
Export	Select and Export the CA certificate. You can do this to import into another system or to view the certificate offline.

Device > Certificate Management > Certificate Profile

- ▲ Device > Certificate Management > Certificate Profile
- ▲ Panorama > Certificate Management > Certificate Profiles

Certificate profiles define user and firewall authentication for Captive Portal, GlobalProtect, site-to-site IPSec VPN, and web interface access to firewalls and Panorama. The profiles specify which certificate authority (CA) certificates to use for verifying client certificates, how to verify certificate revocation status, and how that status constrains access. Configure a certificate profile for each application.

Certificate Profile Setting	Description
Name	(Required) 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: <ul style="list-style-type: none"> • 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	(Required) Click Add and select a CA Certificate to assign to the profile. Optionally, if the firewall uses Online Certificate Status Protocol (OCSP) to verify certificate revocation status, configure the following fields to override the default behavior. For most deployments, these fields do not apply. <ul style="list-style-type: none"> • By default, the firewall uses the OCSP responder URL (see settings to Device > Certificate Management > OCSP Responder). To override the OCSP responder 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 this option to use a certificate revocation list (CRL) to verify the revocation status of certificates.

Certificate Profile Setting	Description
Use OCSP	Select this option to use OCSP to verify the revocation status of certificates.  If you select both OCSP and CRL, the firewall first tries OCSP and only falls back to the CRL method if the OCSP responder is unavailable.
CRL Receive Timeout	Specify the interval (1-60 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.
Block session if certificate status is unknown	Select this option if you want the firewall to block sessions when the OCSP or CRL service returns a certificate revocation status of <i>unknown</i> . Otherwise, the firewall proceeds with the session.
Block sessions if certificate status cannot be retrieved within timeout	Select this option if you want the firewall to block sessions after it registers an OCSP or CRL request timeout. Otherwise, the firewall proceeds with the session.
Block sessions if the certificate was not issued to the authenticating device	(GlobalProtect only) Select this option if you want the firewall to block sessions when the serial number attribute in the subject of the client certificate does not match the host ID that the GlobalProtect agent reports for the client endpoint. Otherwise, the firewall allows the sessions. This option applies only to GlobalProtect certificate authentication .

Device > Certificate Management > OCSP Responder

Select **Device > Certificate Management > OCSP Responder** to define an Online Certificate Status Protocol (OCSP) responder (server) to verify the revocation status of certificates.

Besides adding an OCSP responder, enabling OCSP requires the following tasks:

- Enable communication between the firewall and the OCSP server. Select **Device > Setup > Management**, select **HTTP OCSP** in Management Interface Settings, and then click **OK**.
- If the firewall will decrypt outbound SSL/TLS traffic, optionally configure it to verify the revocation status of destination server certificates. Select **Device > Setup > Sessions**, click **Decryption Certificate Revocation Settings**, select **Enable** in the OCSP settings, enter the **Receive Timeout** (the interval after which the firewall stops waiting for an OCSP response), and then click **OK**.
- Optionally, to configure the firewall as an OCSP responder, add an Interface Management profile to the interface used for OCSP services. First, select **Network > Network Profiles > Interface Mgmt**, click **Add**, select **HTTP OCSP**, and then click **OK**. Second, select **Network > Interfaces**, click the name of the interface that the firewall will use for OCSP services, select **Advanced > Other info**, select the Interface Management profile you configured, and then click **OK** and **Commit**.

OCSP Responder Setting	Description
Name	Enter a name to identify the responder (up to 31 characters). The name is case-sensitive. It must be unique and use only letters, numbers, spaces, hyphens, and underscores.
Location	Select the scope in which the responder is available. In the context of a firewall that has more than one virtual system (vsys), select a vsys or select Shared (all virtual systems). In any other context, you can't select the Location ; its value is predefined as Shared. After you save the responder, you can't change its Location .
Host Name	Enter the host name (recommended) or IP address of the OCSP responder. From this value, PAN-OS automatically derives a URL and adds it to the certificate being verified. If you configure the firewall as an OCSP responder, the host name must resolve to an IP address in the interface that the firewall uses for OCSP services.

Device > Certificate Management > SSL/TLS Service Profile

- ▲ Device > Certificate Management > SSL/TLS Service Profile
- ▲ Panorama > Certificate Management > SSL/TLS Service Profile

SSL/TLS service profiles specify a server certificate and a protocol version or range of versions for firewall 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 client systems requesting the services.



In the client systems that request firewall services, the certificate trust list (CTL) must include the certificate authority (CA) certificate that issued the certificate specified in the SSL/TLS service profile. Otherwise, users will see a certificate error when requesting firewall services. Most third-party CA certificates are present by default in client browsers. If an enterprise or firewall-generated CA certificate is the issuer, you must deploy that CA certificate to the CTL in client browsers.

- To add a profile, click **Add**, complete the fields in the following table, 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**.

The following table describes SSL/TLS service profile settings.

SSL/TLS Service Profile Setting	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 option to make the profile available on all virtual systems. By default, this option 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 server certificate to associate with the profile. See Manage Firewall and Panorama Certificates . ⚠ Do not use certificate authority (CA) certificates for SSL/TLS services; use only signed certificates.
Min Version	Select the earliest (Min Version) and latest (Max Version) version of TLS that services can use: TLSv1.0 , TLSv1.1 , TLSv1.2 , or Max (the latest available version).
Max Version	⚠ Client certificates that are used when requesting firewall services that rely on TLSv1.2 cannot have SHA384 (in releases before PAN-OS 7.1.8) or SHA512 as a digest algorithm. The client certificates must use a lower digest algorithm or you must limit the Max Version to TLSv1.1 for the services.

Device > Certificate Management > SCEP

The simple certificate enrollment protocol (SCEP) provides a mechanism for issuing a unique certificate to endpoints, gateways, and satellite devices. Select **Device > Certificate Management > SCEP** to create an SCEP configuration.

To start a new SCEP configuration, click **Add** and then complete the following fields.

SCEP Setting	Description
Name	Specify a descriptive Name to identify this SCEP configuration, such as <i>SCEP_Example</i> . This name distinguishes a SCEP profile from other instances that you might have among the configuration profiles.
Location	Select a Location for the profile if the system has multiple virtual systems. The location identifies where the SCEP configuration is available.
One Time Password (Challenge)	
SCEP Challenge	<p>(Optional) To make SCEP-based certificate generation more secure, you can configure a SCEP challenge-response mechanism (a one-time password (OTP)) between the public key infrastructure (PKI) and the portal for each certificate request.</p> <p> After you configure this mechanism, its operation is invisible, and no further input from you is necessary.</p> <p>The challenge mechanism that you select determines the source of the OTP. If you select Fixed, you copy the enrollment challenge password from the PKI's SCEP server and enter the string in the portal's Password dialog that displays when configured as Fixed. Each time the portal requests a certificate, it uses this password to authenticate with the PKI. If you select Dynamic, you enter the username and password of your choice (possibly the credentials of the PKI administrator) and the SCEP Server URL where the portal-client submits these credentials. This username and password remains the same while the SCEP server transparently generates an OTP password for the portal upon each certificate request. (You can see this OTP change after a screen refresh in "The enrollment challenge password is" field upon each certificate request.) The PKI transparently passes each new password to the portal, which then uses the password for its certificate request.</p> <p> To comply with the U.S. Federal Information Processing Standard (FIPS), select Dynamic, specify a Server URL that uses HTTPS, and enable SCEP Server SSL Authentication. (FIPS-CC operation is indicated on the firewall login page and in the firewall status bar.)</p>
Configuration	
Server URL	Enter the URL at which the portal requests and receives client certificates from the SCEP server. For example: <code>http://<hostname or IP>/certsrv/mscep/</code>
CA-IDENT Name	Enter a string to identify the SCEP server. Maximum length is 255 characters.

SCEP Setting	Description
Subject	<p>Configure the Subject to include identifying information about the device and optionally user and provide this information in the certificate signing request (CSR) to the SCEP server.</p> <p>When used to request client certificates for endpoints, the endpoint sends identifying information about the device that includes its host ID value. The host ID value varies by device type, either GUID (Windows) MAC address of the interface (Mac), Android ID (Android devices), UDID (iOS devices), or a unique name that GlobalProtect assigns (Chrome). When used to request certificates for satellite devices, the host ID value is the device serial number.</p> <p>To specify additional information in the CSR, enter the Subject name. The subject must be a distinguished name in the <code><attribute>=<value></code> format and must include the common name (CN) key. For example:</p> <pre>O=acme, CN=acmescep</pre> <p>There are two ways to specify the CN:</p> <ul style="list-style-type: none"> • Token-based CN (Recommended)—Enter one of the supported tokens <code>\$USERNAME</code>, <code>\$EMAILADDRESS</code>, or <code>\$HOSTID</code>. Use the username or email address variable to ensure that the portal requests certificates for a specific user. To request certificates for the device only, specify the <code>hostid</code> variable. When the GlobalProtect portal pushes the SCEP settings to the agent, the CN portion of the subject name is replaced with the actual value (username, <code>hostid</code>, or email address) of the certificate owner. For example: <pre>O=acme, CN=\$HOSTID</pre> • Static CN—The CN you specify will be used as the subject for all certificates issued by the SCEP server. For example: <pre>O=acme, CN=acmescep</pre>
Subject Alternative Name Type	<p>After you select a type other than None, a dialog displays for you to enter the appropriate value.</p> <ul style="list-style-type: none"> • RFC 822 Name—Enter the email name in a certificate's subject or Subject Alternative Name extension. • DNS Name—Enter the DNS name used to evaluate certificates. • Uniform Resource Identifier (URI)—Enter the name of the URI resource from which the client obtains the certificate.
Cryptographic Settings	<ul style="list-style-type: none"> • Number of Bits—Select the key's Number of Bits for the certificate. If the firewall is in FIPS-CC mode, the generated keys must be at least 2,048 bits. (FIPS-CC operation is indicated on the firewall login page and the firewall status bar.) • Digest—Select the Digest algorithm for the certificate—SHA1, SHA256, SHA384, or SHA512. If the firewall is in FIPS-CC mode, you must select SHA256, SHA384, or SHA512 as the Digest algorithm.
Use as digital signature	Select this option to configure the endpoint to use the private key in the certificate to validate a digital signature.
Use for key encipherment	Select this option to configure the client endpoint to use the private key in the certificate to encrypt data exchanged over the HTTPS connection established with the certificates issued by the SCEP server.

SCEP Setting	Description
CA Certificate Fingerprint	<p>(Optional) To ensure that the portal connects to the correct SCEP server, enter the CA Certificate Fingerprint. Obtain this fingerprint from the SCEP server interface in the Thumbprint field.</p> <p>Log in to the SCEP server's administrative user interface (for example, at <code>http://<hostname or IP>/CertSrv/mscep_admin/</code>). Copy the thumbprint and enter it in CA Certificate Fingerprint.</p>
SCEP Server SSL Authentication	To enable SSL, select the SCEP server's root CA Certificate . Optionally, you can enable mutual SSL authentication between the SCEP server and the GlobalProtect portal by selecting a Client Certificate .

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.

Custom Response 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. Select Objects > Security Profiles > File Blocking .
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 the firewall will decrypt SSL sessions for inspection.
URL Filtering and Category Match Block Page	Access blocked by a URL filtering profile or because the URL category is blocked by a security policy.
URL Filtering Continue and Override Page	Page with initial block policy that allows users to bypass the block. For example, a user who thinks the page was blocked inappropriately can click Continue to proceed to the page. With the override page, a password is required for the user to override the policy that blocks this URL. See the URL Admin Override section for instructions on setting the override password.
URL Filtering Safe Search Enforcement Block Page	Access blocked by a security policy 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 for **Response Pages**.

- To import a custom HTML response page, click the link of the page type you would like to change and then click import/export. Browse to locate the page. A message is displayed to indicate whether the import succeeded. For the import to be successful, the file must be in HTML format.

- To export a custom HTML response page, click **Export** for the type of page. Select whether to open the file or save it to disk and, if appropriate, select **Always use the same option**.
- To enable or disable the **Application Block** page or **SSL Decryption Opt-out** pages, click **Enable** for the type of page. Select or deselect **Enable**, as appropriate.
- To use the default response page instead of a previously uploaded custom page, delete the custom block page and commit. This will set the default block page as the new active page.

Device > Log Settings

Select **Device > Log Settings** to configure alarms, clear logs, or enable log forwarding to Panorama and external services.

- [Select Log Forwarding Destinations](#)
- [Define Alarm Settings](#)
- [Clear Logs](#)

Select Log Forwarding Destinations

Use this page to forward logs to the following destinations:

- **Panorama**—To specify the address of the Panorama management server, see [Panorama Settings: Device > Setup > Management](#).
- **SNMP trap server**—To define the SNMP trap servers, see [Device > Server Profiles > SNMP Trap](#).
- **Syslog server**—To define the syslog servers, see [Device > Server Profiles > Syslog](#).
- **Email server**—To define the email recipients and servers, see [Device > Server Profiles > Email](#).



To configure destinations for Traffic, Threat and WildFire Submissions logs, see [Objects > Log Forwarding](#).

You can forward the following log types.

Log Type	Description
Config logs	Record configuration changes to firewall or Panorama. Each entry includes the date and time, the administrator username, the IP address from where the change was made, the type of client (XML, 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 logs	Show system events such as HA failures, link status changes, and administrators logging in and out of the firewall. You can select a different destination for each log severity level: <ul style="list-style-type: none">• 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.

Log Type	Description
Correlation logs	<p>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 Monitor > Automated Correlation Engine.</p> <p> You cannot forward Correlation logs from firewalls to Panorama. Panorama generates Correlation logs based on the firewall logs it receives.</p> <p>You can select a different destination for each log severity level:</p> <ul style="list-style-type: none"> • 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 logs	<p>Display traffic flows that match a HIP object or HIP profile. Select Objects > GlobalProtect > HIP Objects to set up a HIP object or select Objects > GlobalProtect > HIP Profiles to create a HIP profile.</p>

Define Alarm Settings

Use the Alarm Settings to configure [Alarms](#) for the CLI and the web interface. You can configure notifications for the following events:

- A security rule (or group of rules) has been matched at a specified threshold and within a specified time interval.
- Encryption/Decryption failure threshold is met.
- The Log database for each log type is nearing full; the quota by default is set to notify when 90% of the available disk space is used. Configuring alarms allows to take action before the disk is full, and logs are purged.

When you enable alarms, you can view the current list by clicking [Alarms](#) () in the bottom of the web interface.

To add an alarm, edit the alarm settings.

Alarm Log Setting	Description
Enable Alarms	Enable alarms based on the events listed on this page. Alarms is visible only when you Enable Alarms .
Enable CLI Alarm Notifications	Enable CLI alarm notifications whenever alarms occur.
Enable Web Alarm Notifications	Open a window to display alarms on user sessions, including when they occur and when they are acknowledged.
Enable Audible Alarms	An audible alarm tone will play every 15 seconds on the administrator's computer when the administrator is logged into the web interface and unacknowledged alarms exist. The alarm tone will play until the administrator acknowledges all alarms. To view and acknowledge alarms, click Alarms . This feature is only available when in the firewall is in FIPS-CC mode.
Encryption/Decryption Failure Threshold	Specify the number of encryption/decryption failures after which an alarm is generated.
Log 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.

Alarm Log Setting	Description
Selective Audit	<p>The selective audit options are only available when the firewall is in FIPS-CC mode.</p> <p>Specify the following settings:</p> <ul style="list-style-type: none"> • FIPS-CC Specific Logging—Enables verbose logging required for Common Criteria (CC) compliance. • Packet Drop Logging—Logs packets dropped by the firewall. • SUPPRESS Login Success Logging—Stops logging of successful administrator logins to the firewall. • SUPPRESS Login Failure Logging—Stops logging of failed administrator logins to the firewall. • TLS Session Logging—Logs the establishment of TLS sessions. • CA (OCSP/CRL) Session Establishment Logging—Logs session establishment between the firewall and a certificate authority when the firewall sends a request to check certificate revocation status using the Online Certificate Status Protocol or a Certificate Revocation List server request. (Disabled by default.) • IKE Session Establishment Logging—Logs IPSec IKE session establishment when the VPN gateway on the firewall authenticates with a peer. The peer can be a Palo Alto Networks firewalls or another security device used to initiate and terminate VPN connections. The interface name that is specified in the log is the interface that is bound to the IKE gateway. The IKE gateway name is also displayed if applicable. Disabling this option stops logging of all IKE logging events. (Enabled by default.) • Suppressed Administrators—Stops logging of changes that the listed administrators make to the firewall configuration.

Clear Logs

You can clear logs on the firewall when you Manage Logs on the Log Settings page. Click the log type you want to clear and click **Yes** to confirm the request.



To automatically delete logs and reports, you can configure expiration periods. For details, see [Logging and Reporting Settings](#).

Device > Server Profiles

- ▲ [Device > Server Profiles > SNMP Trap](#)
- ▲ [Device > Server Profiles > Syslog](#)
- ▲ [Device > Server Profiles > Email](#)
- ▲ [Device > Server Profiles > NetFlow](#)
- ▲ [Device > Server Profiles > RADIUS](#)
- ▲ [Device > Server Profiles > TACACS+](#)
- ▲ [Device > Server Profiles > LDAP](#)
- ▲ [Device > Server Profiles > Kerberos](#)
- ▲ [Device > Server Profiles > DNS](#)

Device > Server Profiles > SNMP Trap

- ▲ 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). Select **Device > Server Profiles > SNMP Trap** or **Panorama > Server Profiles > SNMP Trap** to configure the server profile that enables the firewall or Panorama to send traps to the SNMP managers. To enable SNMP GET messages (statistics requests from an SNMP manager), see [Enable SNMP Monitoring](#).

After creating the server profile, you must specify which log types will trigger the firewall to send SNMP traps ([Device > Log Settings](#)). For a list of the MIBs that you must load into the SNMP manager so it can interpret traps, see [Supported MIBs](#).



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

SNMP Trap Server Profile Setting	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 <i>community</i> 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).

SNMP Trap Server Profile Setting	Description
For SNMP V3	
Name	Specify a name for the SNMP manager. The name can have up to 31 characters that are alphanumeric, periods, underscores, or hyphens.
SNMP Manager	Specify the FQDN or IP address of the SNMP manager.
User	Specify a username to identify the SNMP user account (up to 31 characters). The username you configure on the firewall must match the username configured on the SNMP manager.
EngineID	Specify the engine ID of the firewall. When an SNMP manager and the firewall authenticate to each other, trap messages use this value to uniquely identify the firewall. If you leave the field blank, the messages use the firewall serial number as the EngineID . If you enter a value, it must be in hexadecimal format, prefixed with 0x, and with another 10-128 characters to represent any number of 5-64 bytes (2 characters per byte). For firewalls in a high availability (HA) configuration, leave the field blank so that the SNMP manager can identify which HA peer sent the traps; otherwise, the value is synchronized and both peers will use the same EngineID .
Auth Password	Specify the authentication password of the SNMP user. The firewall uses the password to authenticate to the SNMP manager. The firewall uses Secure Hash Algorithm (SHA-1 160) to encrypt the password. The password must be 8-256 characters and all characters are allowed.
Priv Password	Specify the privacy password of the SNMP user. The firewall uses the password and Advanced Encryption Standard (AES-128) to encrypt traps. The password must be 8-256 characters and all characters are allowed.

Device > Server Profiles > Syslog

- ▲ Device > Server Profiles > Syslog
- ▲ Panorama > Server Profiles > Syslog

To forward System, Config, Traffic, Threat, HIP Match, or Correlation logs as syslog messages, define one or more syslog server profiles by clicking **Add** and specifying the New Syslog Server fields.



- To select the syslog server profile for System, Config, HIP Match, and Correlation logs, see [Device > Log Settings](#).
- To select the syslog server profile for Traffic, Threat, and WildFire logs, see [Objects > Log Forwarding](#).
- You cannot delete a server profile that the firewall uses in any System or Config log settings or Log Forwarding profile.

Syslog Server Setting	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	<p>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.</p> <p>For details on the fields that can be used for custom logs, see Device > Server Profiles > Email.</p>

Syslog Server Setting	Description
Escaping	Specify escape sequences. Escaped characters is a list of all the characters to be escaped without spaces.

Device > Server Profiles > Email

- ▲ Device > Server Profiles > Email
- ▲ Panorama > Server Profiles > Email

To forward logs as email notifications, define an email server profile by clicking **Add** and specifying the Email Notification Settings.



- To select the email server profile for System, Config, HIP Match, and Correlation logs, see [Device > Log Settings](#).
- To select the email server profile for Traffic, Threat, and WildFire logs, see [Objects > Log Forwarding](#).
- You can also [Monitor > PDF Reports > Email Scheduler](#).
- You cannot delete a server profile that the firewall uses in any System or Config log settings or Log Forwarding profile.

Email Notification Setting	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 <code>From</code> field of the email.
From	Enter the From email address, such as <code>security_alert@company.com</code> .
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.

Device > Server Profiles > NetFlow

▲ Device > Server Profiles > Netflow

Palo Alto Networks firewalls can export statistics about the IP traffic on their interfaces as NetFlow fields to a NetFlow collector. The NetFlow collector is a server you use to analyze network traffic for security, administration, accounting and troubleshooting. All Palo Alto Networks firewalls support NetFlow Version 9 except the PA-4000 Series firewall and PA-7000 Series firewalls. The firewalls support only unidirectional NetFlow, not bidirectional. The firewalls perform NetFlow processing on all IP packets on the interfaces and do not support sampled NetFlow. You can export NetFlow records for Layer 3, Layer 2, virtual wire, tap, VLAN, loopback, and tunnel interfaces. For aggregate Ethernet interfaces, you can export records for the aggregate group but not for individual interfaces within the group. The firewalls support standard and enterprise (PAN-OS specific) NetFlow templates, which NetFlow collectors use to decipher the NetFlow fields. The firewalls select a template based on the type of exported data: IPv4 or IPv6 traffic, with or without NAT, and with standard or enterprise-specific fields.

To [configure NetFlow exports](#), Add a NetFlow server profile to specify which NetFlow servers will receive the exported data and to specify export parameters. After you assign the profile to an interface (see [Network > Interfaces](#)), the firewall exports NetFlow data for all traffic on that interface to the specified servers.

Netflow Setting	Description
Name	Enter a name for the Netflow server profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Template Refresh Rate	The firewall periodically refreshes NetFlow templates to re-evaluate which one to use (in case the type of exported data changes) and to apply any changes to the fields in the selected template. Specify the rate at which the firewall refreshes NetFlow templates in Minutes (range is 1 to 3,600; default is 30) and Packets (exported records—range is 1 to 600; default is 20), according to the requirements of your NetFlow collector. The firewall refreshes the template after either threshold is passed. The required refresh rate depends on the NetFlow collector. If you add multiple NetFlow collectors to the server profile, use the value of the collector with the fastest refresh rate.
Active Timeout	Specify the frequency (in minutes) at which the firewall exports data records for each session (range is 1–60; default is 5). Set the frequency based on how often you want the NetFlow collector to update traffic statistics.
PAN-OS Field Types	Export PAN-OS specific fields for App-ID and the User-ID service in Netflow records.
Servers	
Name	Specify a name to identify the server (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Server	Specify the hostname or IP address of the server. You can add a maximum of two servers per profile.
Port	Specify the port number for server access (default 2055).

Device > Server Profiles > RADIUS

- ▲ Device > Server Profiles > RADIUS
- ▲ Panorama > Server Profiles > RADIUS

Select **Device > Server Profiles > RADIUS** or **Panorama > Server Profiles > RADIUS** to [configure](#)  settings for the RADIUS servers that authentication profiles reference.

RADIUS Server Setting	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 option to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, this option appears only if the Location is Shared .
Timeout	Enter an interval in seconds after which an authentication request times out (range is 1–120; default is 3).
Retries	Enter the number of automatic retries following a timeout before the request fails (range is 1–5; default is 3).
Servers	Configure information for each server in the preferred order. <ul style="list-style-type: none"> • Name—Enter a name to identify the server. • RADIUS Server—Enter the server IP address or FQDN. • Secret/Confirm Secret—Enter and confirm a key to verify and encrypt the connection between the firewall and the RADIUS server. • Port—Enter the server port (range is 1–65,535; default is 1812) for authentication requests.

Device > Server Profiles > TACACS+

- ▲ Device > Server Profiles > TACACS+
- ▲ Panorama > Server Profiles > TACACS+

Select **Device > Server Profiles > TACACS+** or **Panorama > Server Profiles > TACACS+** to [configure](#) settings for the Terminal Access Controller Access-Control System Plus (TACACS+) servers that authentication profiles reference (see [Device > Authentication Profile](#)).

TACACS+ Server Setting	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 option to specify that only administrator accounts can use the profile for authentication. For multi-vsys firewalls, this option appears only if the Location is Shared .
Timeout	Enter an interval in seconds after which an authentication request times out (range is 1–20; default is 3).
Use single connection for all authentication	Select this option to use the same TCP session for all authentications. This option improves performance by avoiding the processing required to initiate and tear down a separate TCP session for each authentication event.
Servers	Click Add and specify the following settings for each TACACS+ server: <ul style="list-style-type: none"> • Name—Enter a name to identify the server. • TACACS+ Server—Enter the IP address or FQDN of the TACACS+ server. • Secret/Confirm Secret—Enter and confirm a key to verify and encrypt the connection between the firewall and the TACACS+ server. • Port—Enter the server port (default is 49) for authentication requests.

Device > Server Profiles > LDAP

- ▲ Device > Server Profiles > LDAP
- ▲ Panorama > Server Profiles > LDAP

Select **Device > Server Profiles > LDAP** or **Panorama > Server Profiles > LDAP** to configure  settings for the LDAP servers that authentication profiles reference (see [Device > Authentication Profile](#)).

LDAP Server Setting	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 option to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, this option appears only if the Location is Shared .
Servers	For each 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.
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 1-3,600; default is 60).
Require SSL/TLS secured connection	<p>Select this option if you want the firewall to use SSL or TLS for communications with the directory server. The protocol depends on the server port:</p> <ul style="list-style-type: none"> • 389 (default)—TLS (Specifically, the firewall uses the Start TLS operation, which upgrades the initial plaintext connection to TLS.) • 636—SSL • Any other port—The firewall first attempts to use TLS. If the directory server doesn't support TLS, the firewall falls back to SSL. <p>This option is selected by default.</p>

LDAP Server Setting	Description
Verify Server Certificate for SSL sessions	<p>Select this option (it is cleared by default) if you want the firewall to verify the certificate that the directory server presents for SSL/TLS connections. The firewall verifies the certificate in two respects:</p> <ul style="list-style-type: none">• The certificate is trusted and valid. For the firewall to trust the certificate, its root certificate authority (CA) and any intermediate certificates must be in the certificate store under Device > Certificate Management > Certificates > Device Certificates.• The certificate name must match the host Name of the LDAP server. The firewall first checks the certificate attribute Subject AltName for matching, then tries the attribute Subject DN. If the certificate uses the FQDN of the directory server, you must use the FQDN in the LDAP Server field for the name matching to succeed. <p>If the verification fails, the connection fails. To enable this verification, you must also select Require SSL/TLS secured connection.</p>

Device > Server Profiles > Kerberos

- ▲ Device > Server Profiles > Kerberos
- ▲ Panorama > Server Profiles > Kerberos

Select **Device > Server Profiles > Kerberos** or **Panorama > Server Profiles > Kerberos** to configure a server profile that enables users to natively authenticate to an Active Directory domain controller or a Kerberos V5-compliant authentication server. After configuring a Kerberos server profile you can assign it to an authentication profile, and then [test](#) the Kerberos authentication profile.



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

Kerberos Server Setting	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 option to specify that only administrator accounts can use the profile for authentication. For firewalls that have multiple virtual systems, this option appears only if the Location is Shared .
Servers	For each Kerberos server, click Add and specify the following settings: <ul style="list-style-type: none">• Name—Enter a name for the server.• Kerberos Server—Enter the server IPv4 address or FQDN.• Port—Enter an optional port (range is 1–65,535; default is 88) for communication with the server.

Device > Server Profiles > DNS

To simplify configuration for a virtual system, a DNS server profile allows you to specify the virtual system that is being configured, an inheritance source or the primary and secondary DNS addresses for DNS servers, and the source interface and source address (service route) that will be used in packets sent to the DNS server. The source interface and source address are used as the destination interface and destination address in the reply from the DNS server.

A DNS server profile is for a virtual system only; it is not for the global Shared location.

DNS Server Profile Setting	Description
Name	Name the DNS Server profile.
Location	Select the virtual system to which the profile applies.
Inheritance Source	Select None if the DNS server addresses are not inherited. Otherwise, specify the DNS server from which the profile should inherit settings.
Check inheritance source status	Click to see the inheritance source information.
Primary DNS	Specify the IP address of the primary DNS server.
Secondary DNS	Specify the IP address of the secondary DNS server.
Service Route IPv4	Select this option if you want to specify that packets going to the DNS server are sourced from an IPv4 address.
Source Interface	Specify the source interface that packets going to the DNS server will use.
Source Address	Specify the IPv4 source address from which packets going to the DNS server are sourced.
Service Route IPv6	Select this option if you want to specify that packets going to the DNS server are sourced from an IPv6 address.
Source Interface	Specify the source interface that packets going to the DNS server will use.
Source Address	Specify the IPv6 source address from which packets going to the DNS server are sourced.

Device > Local User Database > Users

You can set up a local database on the firewall to store authentication information for firewall administrators, Captive Portal end users, and end users who authenticate to a GlobalProtect portal and GlobalProtect gateway. Local database authentication requires no external authentication service; you perform all account management on the firewall. After creating the local database and (optionally) assigning the users to groups (see [Device > Local User Database > User Groups](#)), you can [Device > Authentication Profile](#) based on the local database.



You cannot [Device > Password Profiles](#) for administrative accounts that use local database authentication.

To **Add** a local user to the database, complete the following fields.

Local User Setting	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: <ul style="list-style-type: none">• Password—Enter and confirm a password for the user.• Password Hash—Enter a hashed password string. This can be useful if, for example, you want to reuse the credentials for an existing Unix account but don't know the plaintext password, only the hashed password. The firewall accepts any string of up to 63 characters regardless of the algorithm used to generate the hash value. The operational CLI command <code>request password-hash password</code> uses the MD5 algorithm when the firewall is in normal mode and the SHA256 algorithm when the firewall is in CC/FIPS mode.  Any Minimum Password Complexity parameters you set for the firewall (Device > Setup > Management) do not apply to accounts that use a Password Hash.
Enable	Select this option to activate the user account.

Device > Local User Database > User Groups

Select **Device > Local User Database > User Groups** to add user group information to the local database.

Local User Group Setting	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.

Device > Scheduled Log Export

You can **schedule exports of logs** and save them in CSV format to a File Transfer Protocol (FTP) server or use Secure Copy (SCP) to securely transfer data between the firewall and a remote host. Log profiles contain the schedule and FTP server information. For example, a profile may specify that the previous day's logs are collected each day at 3AM and stored on a particular FTP server.

Click **Add** and fill in the following details.

Scheduled Log Export Setting	Description
Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. You cannot change the name after the profile is created.
Description	Enter an optional description (up to 255 characters).
Enable	Select this option to enable the scheduling of log exports.
Log Type	Select the type of log (traffic, threat, 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: <ul style="list-style-type: none"> FTP—This protocol is not secure. SCP—This protocol is secure. After completing the remaining fields, you must click Test SCP server connection to test connectivity between the firewall and the SCP server and you must verify and accept the host key of the SCP server.
Hostname	Enter the host name or IP address of the FTP server that will be used for the export.
Port	Enter the port number that the FTP server will use. Default is 21.
Path	Specify the path located on the FTP server that will be used to store the exported information.
Enable FTP Passive Mode	Select this option to use passive mode for the export. By default, this option is selected.
Username	Enter the user name for access to the FTP server. Default is anonymous.
Password / Confirm Password	Enter the password for access to the FTP server. A password is not required if the user is anonymous.
Test SCP server connection (SCP protocol only)	If you set the Protocol to SCP , you must click this button to test connectivity between the firewall and the SCP server and then verify and accept the host key of the SCP server.  If you use a Panorama template to configure the log export schedule, you must perform this step after committing the template configuration to the firewalls. After the template commit, log in to each firewall, open the log export schedule, and click Test SCP server connection .

Device > Software

▲ Device > Software

Select **Device > Software** 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 firewall, 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. (Select **Device > Setup > Operations** 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 firewall 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 firewall checks the signature before installing a new version. If the date setting on the firewall is not current, the firewall might perceive the software signature to be erroneously in the future and will display the following message:

Decrypt failed: GnuPG edit non-zero, with code 171072 Failed to load into PAN software manager.

The following table provides help for using the **Software** page.

Software Options 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.

Software Options Field	Description
Action	<p>Indicates the current action you can take for the corresponding software image as follows:</p> <ul style="list-style-type: none"> • Download—The corresponding software version is available on the Palo Alto Networks Update Server; click to Download an available software version. • Install—The corresponding software version has been downloaded or uploaded to the firewall; click to Install the software. A reboot is required to complete the upgrade process. • Reinstall—The corresponding software version was installed previously; click to Reinstall the same version.
Release Notes	Provides a link to the release notes for the corresponding software update. This link is only available for updates that you download from the Palo Alto Networks Update Server—it is not available for uploaded updates.
	Removes the previously downloaded or uploaded software image from the firewall. You would only want to delete the base image for older releases that will not need upgrading. For example, if you are running 7.0, you can remove the base image for 6.1 unless you think you might need to downgrade.
Check Now	Checks whether a new software update is available from Palo Alto Networks.
Upload	<p>Imports a software update image from a computer that the firewall can access. Typically, you perform this action if the firewall doesn't have Internet access, which is required when downloading updates from the Palo Alto Networks Update Server. For uploads, use an Internet-connected computer to visit the Palo Alto Networks website, download the software image from the Support site (Software Updates), download the update to your computer, select Device > Software on the firewall and Upload the software image. In a high availability (HA) configuration, you can select Sync To Peer to push the imported software image to the HA peer. After the upload, the Software page displays the same information (for example, version and size) and Install/Reinstall options for uploaded and downloaded software. Release Notes option is not active for uploaded software.</p>

Device > Dynamic Updates

- ▲ 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 firewalls 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 public cloud. WildFire signature updates are made available every five minutes. You can set the firewall to check for new updates as frequently as every minute to ensure that the firewall retrieves the latest WildFire signatures within a minute of availability. Without the WildFire subscription, you must wait 24 to 48 hours for the WildFire signatures to roll into the Applications and Threat update. Select **Device > Setup > WildFire** to enable **WildFire Public Cloud** analysis.
- **WF-Private**—Provides near real-time malware and antivirus signatures created as a result of the analysis done by a WF-500 appliance. To receive content updates from a WF-500 appliance, the firewall and appliance must both be running PAN-OS 6.1 or a later release and the firewall must be configured to forward files and email links to the WildFire Private Cloud. Select **Device > Setup > WildFire** to enable WildFire Private Cloud 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 [Schedule Dynamic Content Updates](#).

Dynamic Updates Option	Description
Version	Lists the versions that are currently available on the Palo Alto Networks Update Server. To check if a new software release is available from Palo Alto Networks, click Check Now . The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list.
Last checked	Displays the date and time that the firewall last connected to the update server and checked if an update was available.
Schedule	<p>Allows you to schedule the frequency for retrieving updates. You can define how often and when the dynamic content updates occur—the Recurrence and time—and whether to Download Only or to Download and Install the scheduled updates on the firewall.</p> <p>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 Apps, Threats on the Dynamic Updates page or select Objects > Applications).</p> <p>In rare instances, there can be an error in a content update. You can reduce the chance of being impacted by an unexpected issue by delaying updates to new versions until content updates are released for a specified number of hours. To delay updates to new content versions, add a Threshold (hours) value. For example, if you specify a threshold of 48 hours and your firewall is configured to download and install updates every hour, the firewall will query the update server every hour but will not download and install a new update until that update remains available for more than 48 hours.</p>
File Name	List the filename; it includes the content version information.
Features	<p>Lists what type of signatures the content version might include. For Applications and Threats content release versions, this field might display an option to review Apps, Threats. Click this option to view new application signatures made available since the last content release version installed on the firewall. You can also use the New Applications dialog to Enable/Disable new applications. You might choose to disable a new application included in a content release if you want to avoid any policy impact from an application being uniquely identified (an application might be treated differently before and after a content installation if a previously unknown application is identified and categorized differently).</p>
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.

Dynamic Updates Option	Description
Currently Installed	A check mark in this column indicates that the corresponding content release version is currently running on the firewall.
Action	<p>Indicates the current action you can take for the corresponding software image as follows:</p> <ul style="list-style-type: none"> • Download—The corresponding content release version is available on the Palo Alto Networks Update Server; click to Download the content release version. If the firewall does not have access to the Internet, use an Internet-connected computer to go to the Dynamic Updates site to look for and Download the content release version to your local computer. Then manually Upload the software image to the firewall. Additionally, downloading an Application and Threat content release version enables the option to Review Policies that are affected by new application signatures included with the release. • 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 to Install the update. When installing a new Applications and Threats content release version, you are prompted with the option to Disable new apps in content update. This option enables protection against the latest threats, while giving you the flexibility to enable applications after preparing any policy updates, due to the impact of new application signatures (to enable applications you have previously disabled, select Apps, Threats on the Dynamic Updates page or select Objects > Applications). • Revert—The corresponding content release version has been downloaded previously To reinstall the same version, click Revert.
Documentation	Provides a link to the release notes for the corresponding version.
	Remove the previously downloaded content release version from the firewall.
Upload	If the firewall does not have access to the Palo Alto Networks Update Server, you can manually download dynamic updates from the Palo Alto Networks Support site in the Dynamic Updates section. After you download an update to your computer, Upload the update to the firewall. You then select Install From File and select the file you downloaded.
Install From File	After you manually upload an update file to the firewall, use this option to install the file. In the Package Type drop-down, select the type of update you are installing (Application and Threats, Antivirus, or WildFire), click OK , select the file you want to install and then click OK again to start the installation.

Device > Licenses

Select **Device > Licenses** to activate licenses on all firewall 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**—Select to enable purchased subscriptions that require an authorization code and have been activated on the support portal.
- **Activate feature using authorization code**—Select to enable purchased subscriptions that require an authorization code and have not been previously activated on the support portal. Then enter your authorization code, and click **OK**.
- **Manually upload license key**—If the firewall does not have connectivity to the license server and you want to upload license keys manually, download the license key file from <https://support.paloaltonetworks.com>, and save it locally. Click **Manually upload license key**, click **Browse**, select the file, and then click **OK**.
- **Deactivate VM**—This option is available on the VM-Series firewall with the Bring Your Own License model that supports perpetual and term-based licenses; the on-demand license model does not support this functionality.

Click **Deactivate VM** when you no longer need an instance of the VM-Series firewall. It allows you to free up all active licenses—subscription licenses, VM-Capacity licenses, and support entitlements—using this option. The licenses are credited back to your account and you can then apply the licenses on a new instance of a VM-Series firewall, when you need it.

When the license is deactivated, the VM-Series firewall functionality is disabled and the firewall is in an unlicensed state. However, the configuration remains intact.

- Click **Continue Manually** if the VM-Series firewall does not have direct Internet access. The firewall generates a token file. Click **Export license token** to save the token file to your local computer and then reboot the firewall. Log in to the [Palo Alto Networks Support portal](#), select **Assets > Devices**, and **Deactivate VM** to use this token file and complete the deactivation process.
- Click **Continue** to deactivate the licenses on the VM-Series firewall. Click **Reboot Now** to complete the license deactivation process.
- Click **Cancel** if you want to cancel and close the Deactivate VM window.



To enable licenses for URL filtering, you must install the license, download the database, and click **Activate**. If you are using PAN-DB for URL Filtering, you will need to **Download** the initial seed database first and then **Activate**.

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

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.

Device > Support

- ▲ Device > Support
- ▲ Panorama > Support

Select **Device > Support or Panorama > Support** to access support related options. You can view the Palo Alto Networks contact information, view your support expiration date, and view product and security alerts from Palo Alto Networks based on the serial number of your firewall.

Perform any of the following functions on this page:

- **Support**—Use this section to view Palo Alto Networks support contact information, view support status for the firewall 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 support home page, from where you can manage your cases, and a link to register the firewall using your support login.
- **Tech Support File**—Click **Generate Tech Support File** to generate a system file that the support team can use to help troubleshoot issues that you may be experiencing with the firewall. After you generate the file, **Download Tech Support File** and then send it to the Palo Alto Networks Support department.
- **Stats Dump File**—Click **Generate Stats Dump File** to generate a set of XML reports that summarizes network traffic over the last 7 days. After the report is generated, you can **Download Stats Dump File**. The Palo Alto Networks or Authorized Partner systems engineer uses the report to generate 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.
- **Core Files**—If your firewall experiences a system process failure it will generate a core file that contains details about the process and why it failed. Click the **Download Core Files** link to view a list of available core files and then click a core file name to download it. After you download the file, upload it to a Palo Alto Networks support case to obtain assistance in resolving the issue.



Also consider the following:

- 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
- The contents of the core files can be interpreted only by a Palo Alto Networks support engineer.

Device > Master Key and Diagnostics

- ▲ Device > Master Key and Diagnostics
- ▲ Panorama > Master Key and Diagnostics

Select **Device > Master Key and Diagnostics** or **Panorama > Master Key and Diagnostics** to configure the master key that encrypts all passwords and private keys on the firewall or Panorama (such as the RSA key for authenticating administrator access to the CLI).



As a best practice, configure a new master key instead of using the default, periodically change the key, and store the key in a safe location. You can also use a hardware security module to encrypt the master key (see [Device > Setup > HSM](#)).

The only way to restore the default master key is to perform a [factory reset](#).

If you deploy firewalls or Panorama in a high availability (HA) configuration, use the same master key on both HA peers. Otherwise, HA synchronization will not work properly.

If you use Panorama, configure the same master key on Panorama and all managed firewalls. Otherwise, Panorama cannot push configurations to the firewalls.

To configure a master key, edit the Master Key settings using the following table to determine the appropriate values.

Master Key and Diagnostics Setting	Description
Current Master Key	Specify the current master key if one exists.
New Master Key Confirm Master Key	To change the master key, enter a 16-character string and confirm the new key.
Life Time	<p>Specify the number of Days and Hours after which the master key expires (range 1–730 days).</p> <p> You must configure a new master key before the current key expires. If the master key expires, the firewall or Panorama automatically reboots in Maintenance mode. You must then perform a factory reset.</p>
Time for Reminder	<p>Enter the number of Days and Hours before the master key expires when the firewall generates an expiration alarm. The firewall automatically opens the System Alarms dialog to display the alarm. When the Time for Reminder period starts, the firewall also generates a System log with critical severity every hour until you configure a new master key.</p> <p> To ensure the expiration alarm displays, select Device > Log Settings, edit the Alarm Settings, and Enable Alarms.</p>

Master Key and Diagnostics Setting	Description
Stored on HSM	<p>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.</p> <p>The HSM configuration is not synchronized between peer firewalls 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.</p> <p>HSM is not supported the PA-200, PA-500 and PA-2000 Series firewalls.</p>
Common Criteria	In Common Criteria mode, additional options are available to run a cryptographic algorithm self-test and software integrity self-test. A scheduler is also included to specify the times at which the two self-tests will run.



User Identification

▲ Device > User Identification

User Identification (User-ID™) is a Palo Alto Networks® next-generation firewall feature that seamlessly integrates with a range of enterprise directory and terminal services to tie application activity and policies to usernames and groups instead of just IP addresses. Configuring User-ID enables the Application Command Center (ACC), App Scope, reports, and logs to include usernames in addition to user IP addresses. You can configure the following agents to collect IP address-to-username mapping and username-to-group mapping information:

- PAN-OS integrated User-ID agent that runs on the firewall
- Windows-based User-ID agents that are installed on directory servers in your network
- Terminal Services (TS) agents that are installed on Windows/Citrix terminal servers and map usernames to ports on systems where multiple users have the same IP address

You can configure several [methods for collecting user and group mapping information](#), including server monitoring, syslog message parsing, port mapping, XFF headers, and Captive Portal authentication. In a network with multiple firewalls and hundreds of user identification sources or users who rely on local sources for authentication but access remote resources, you can simplify User-ID management by [configuring user mapping redistribution](#) among firewalls.

If the firewall has multiple virtual systems, each virtual system requires a separate User-ID configuration; by default, virtual systems don't share user mapping information, though you can configure them for redistribution. When configuring User-ID, select the virtual system in the **Location** drop-down at the top of the **Device > User Identification** page.

What do you want to know?	See:
Configure the PAN-OS integrated User-ID agent to collect user mapping information for the firewall.	Device > User Identification > User Mapping
Configure the firewall to receive user mapping information from Windows-based User-ID agents or other firewalls behaving as User-ID agents.	Device > User Identification > User-ID Agents
Enforce user-based policy for systems where multiple users have the same IP address.	Device > User Identification > Terminal Services Agents
Enforce policy based on user groups.	Device > User Identification > Group Mapping Settings
Use Captive Portal to enforce policy based on users and groups.	Device > User Identification > Captive Portal Settings
Looking for more?	User-ID

Device > User Identification > User Mapping

Configure the PAN-OS integrated User-ID agent that runs on the firewall to collect user mapping information.

What do you want to know?	See:
Configure the User-ID agent. These settings define the methods that the User-ID agent uses to perform user mapping.	<ul style="list-style-type: none"> Enable the User-ID agent to monitor server logs for user mapping information: Enable Server Monitoring. Ensure that the firewall has the most current user mapping information as users roam and obtain new IP addresses: Configure Cache Timeouts for User Mapping Entries. Enable NT LAN Manager (NTLM) authentication for user mapping through Captive Portal: Enable NTLM Authentication. Enable firewalls to share user and group mapping information to simplify User-ID management: Enable Redistribution of User Mappings Among Firewalls. Configure the User-ID agent to parse syslog messages for user mapping information: Manage Syslog Message Filters. Configure the User-ID agent to omit specific usernames from the mapping process: Manage the User Ignore List. Enable the User-ID agent to use Windows Management Instrumentation (WMI) to probe client systems and monitoring servers for user mapping information: Enable WMI Authentication. Enable the User-ID agent to probe client systems for user mapping information: Enable Client Probing.
Manage access to the servers that the User-ID agent monitors for user mapping information.	Monitor Servers
Manage the subnetworks that the firewall includes or excludes when collecting user mapping information.	Define Subnetworks to Include/Exclude for User Mapping
Looking for more?	Configure User Mapping Using the PAN-OS Integrated User-ID Agent 

Enable WMI Authentication

- ▲ Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > WMI Authentication

To configure the PAN-OS integrated User-ID agent to use [Windows Management Instrumentation \(WMI\)](#) for probing client systems and monitoring Microsoft Exchange servers and domain controllers for user mapping information, complete the following fields.



Because WMI probing trusts data reported back from the endpoint, it is not a recommended method of obtaining User-ID information in a high-security network. If you are using the User-ID agent to parse AD security event logs, syslog messages, or the XML API to obtain User-ID mappings, Palo Alto Networks recommends disabling WMI probing.

If you do choose to use WMI probing, do not enable it on external, untrusted interfaces, as this would cause the agent to send WMI probes containing sensitive information such as the username, domain name, and password hash of the User-ID agent service account outside of your network. This information could potentially be exploited by an attacker to penetrate the network to gain further access.

WMI Authentication Setting	Description
User Name	Enter the domain credentials (User Name and Password) for the account that the firewall will use to access Windows resources. The account requires permissions to perform WMI queries on client computers and to monitor Exchange servers and domain controllers. Use domain\username syntax for the User Name .
Password/Confirm Password	



The [complete procedure](#) to configure the PAN-OS integrated User-ID agent to monitor servers and probe clients requires additional tasks.

Enable Client Probing

- ▲ Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Client Probing

You can configure the User-ID agent to perform WMI [client probing](#) for each client system that the user mapping process identifies. The User-ID agent will periodically probe each learned IP address to verify that the same user is still logged in. When the firewall encounters an IP address for which it has no user mapping, it sends the address to the User-ID agent for an immediate probe. To configure client probing settings, complete the following fields.



The [complete procedure](#) to configure the PAN-OS integrated User-ID agent to probe clients requires additional tasks.

The PAN-OS Integrated User-ID agent doesn't support NetBIOS probing, but the [Windows-based User-ID agent](#) does.

Client Probing Setting	Description
Enable Probing	<p>Select this option to enable WMI probing</p>  <p>Do not enable client probing on high-security networks. Client probing can generate a large amount of network traffic and can pose a security threat when misconfigured. Instead collect user mapping information from more isolated and trusted sources, such as domain controllers and through integrations with Syslog or the XML API, which have the added benefit of allowing you to safely capture user mapping information from any device type or operating system, instead of just Windows clients.</p>
Probe Interval (min)	<p>Enter the probe interval in minutes (range is 1-1440; default is 20). This is the interval between when the firewall finishes processing the last request and when it starts the next request.</p> <p>In large deployments, it is important to set the interval properly to allow time to probe each client that the user mapping process identified. Example, if you have 6,000 users and an interval of 10 minutes, it would require 10 WMI requests per second from each client.</p>  <p>If the probe request load is high, the observed delay between requests might significantly exceed the interval you specify.</p>

Enable Server Monitoring

- ▲ Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Server Monitor

To enable the User-ID agent to collect user mapping information by monitoring the security event logs of servers for logon events, complete the following fields.



If the query load is high for Windows server logs, Windows server sessions, or eDirectory servers, the observed delay between queries might significantly exceed the specified frequency or interval.

The [complete procedure](#) to configure the PAN-OS integrated User-ID agent to monitor servers and probe clients requires additional tasks.

Server Monitoring Setting	Description
Enable Security Log	Select this option to enable security log monitoring on Windows servers.
Server Log Monitor Frequency (sec)	Specify the frequency in seconds at which the firewall will query Windows server security logs for user mapping information (range is 1-3600; default is 2). This is the interval between when the firewall finishes processing the last query and
Enable Session	Select this option to enable monitoring of user sessions on the monitored servers. Each time a user connects to a server, a session is created; the firewall can use this information to identify the user IP address.  Do not select the Enable Session check box. This setting requires that the User-ID agent have an Active Directory account with Server Operator privileges so that it can read all user sessions. Instead, use a Syslog or XML API integration to monitor sources that capture login and logout events for all device types and operating systems (instead of just Windows), such as wireless controllers and NACs.
Server Session Read Frequency (sec)	Specify the frequency in seconds at which the firewall will query Windows server user sessions for user mapping information (range is 1-3600; default is 10). This is the interval between when the firewall finishes processing the last query and when it starts the next query.
Novell eDirectory Query Interval (sec)	Specify the frequency in seconds at which the firewall will query Novell eDirectory servers for user mapping information (range is 1-3600; default is 30). This is the interval between when the firewall finishes processing the last query and when it starts the next query.
Syslog Service Profile	Select an SSL/TLS service profile that specifies the certificate and allowed SSL/TLS versions for communications between the firewall and any syslog senders that the User-ID agent monitors. For details, see Device > Certificate Management > SSL/TLS Service Profile and Manage Syslog Message Filters . If you select None , the firewall uses its predefined, self-signed certificate.

Configure Cache Timeouts for User Mapping Entries

▲ Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Cache

To ensure that the firewall has the most current user mapping information as users roam and obtain new IP addresses, configure timeouts for clearing user mapping entries from the firewall cache.

Cache Setting	Description
Enable User Identification Timeout	Select this option to enable a timeout value for user mapping entries. When the timeout value is reached for an entry, the firewall clears it and collects a new mapping. This ensures that the firewall has the most current information as users roam and obtain new IP addresses.
User Identification Timeout (min)	Set the timeout value in minutes for user mapping entries (range is 1–3,600; default is 45).  If you configure firewalls to redistribute mapping information, each firewall clears the mapping entries it receives based on the timeout you set on that firewall, not on the timeouts set in the forwarding firewalls.

Enable NTLM Authentication

- ▲ Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > NTLM

When a client web request matches a Captive Portal rule with an action set to browser-challenge (see [Policies > Captive Portal](#)), an [NT LAN Manager \(NTLM\)](#) challenge transparently authenticates the client. The firewall then collects user mapping information from the NTLM domain.



As a best practice, choose [Kerberos SSO](#) transparent authentication over NTLM authentication when configuring Captive Portal. Kerberos is a stronger, more robust authentication method than NTLM and it does not require the firewall to have an administrative account to join the domain.

You can enable NTLM authentication processing for only one virtual system per firewall, which you select in the **Location** drop-down at the top of the [User Mapping](#) page.

Optionally, you can use the firewall to perform NTLM authentication processing for other firewalls by adding it as a User-ID agent to those firewalls. For details, see [Configure Access to User-ID Agents](#).

If you use the Windows-based User-ID agent, NTLM responses go directly to the domain controller where you installed the agent. For details, see the **NTLM Authentication** field in [Device > User Identification > Captive Portal Settings](#).



The complete procedures to [configure Captive Portal](#) or [Windows-based User-ID agents](#) require additional tasks.

To configure NTLM authentication processing, complete the following fields.

Field	Description
Enable NTLM authentication processing	Select this option to enable NTLM authentication processing.
NTLM Domain	Enter the NTLM domain name.
Admin User Name (for the NTLM domain)	Enter the administrator account that has access to the NTLM domain. Do not include the domain in the Admin User Name field. Otherwise, the firewall will fail to join the domain.
Password/Confirm Password (for the NTLM domain)	Enter the password for the administrator account that has access to NTLM domain.

Enable Redistribution of User Mappings Among Firewalls

- ▲ Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Redistribution

To enable the firewall you are logged into to function as a User-ID agent for redistributing user mapping information to other firewalls, complete the following fields.



The [complete procedure](#) to configure firewalls to redistribute user mapping information requires additional tasks.

By default, virtual systems on the same firewall don't share user mapping information, though you can configure them for redistribution.

Redistribution Setting	Description
Collector Name	Enter a collector name (up to 255 alphanumeric characters) that identifies the firewall as a User-ID agent for redistributing mapping information.
Pre-Shared Key/Confirm Pre-Shared Key	Enter the pre-shared key (up to 255 alphanumeric characters) that other firewalls will use to establish a secure connection with this firewall to receive user mapping information.

Manage Syslog Message Filters

- ▲ Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Syslog Filters

The User-ID agent uses Syslog Parse profiles to filter [syslog messages](#) for user mapping information. You can create separate profiles for messages from different syslog senders. For a User-ID agent to parse syslog messages, they must meet the following criteria:

- Each message must be a single-line text string. A new line (\n) or a carriage return plus a new line (\r\n) are the delimiters for line breaks.
- The maximum size for individual messages is 2,048 bytes.
- Messages sent over UDP must be contained in a single packet; messages sent over SSL can span multiple packets. A single packet might contain multiple messages.

Palo Alto Networks provides predefined Syslog Parse profiles through [Applications content updates](#). On a firewall with multiple virtual systems, the predefined profiles are global, whereas custom profiles apply only to a single virtual system.

To configure a custom profile, click Add and specify the settings described in the following table. The field descriptions in this table use a login event example from a syslog message with the following format:

```
[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success
User:domain\johndoe_4 Source:192.168.0.212
```



The [complete procedure](#) to configure the User-ID agent to collect user mapping information from a syslog sender requires additional tasks.

If a firewall has predefined profiles that resemble those you want the User-ID agent to use, you can copy the profile settings. To access existing profiles, select **Device > User Identification > User Mapping**, edit the Palo Alto Networks User-ID Agent Setup section, select **Syslog Filters**, and click the name of the Syslog Parse profile that you want to copy.

Field	Description
Syslog Parse Profile	Enter a name for the profile (up to 63 alphanumeric characters).
Description	Enter a description for the profile (up to 255 alphanumeric characters).
Type	<p>Specify the type of parsing to identify successful authentication events:</p> <ul style="list-style-type: none"> Regex Identifier—Use the Event Regex, Username Regex, and Address Regex fields to specify regular expressions (regex) that describe search patterns for identifying and extracting user mapping information from syslog messages. The firewall will use the regex to match authentication events in syslog messages and to match the username and IP address fields within the matching messages. Field Identifier—Use the Event String, Username Prefix, Username Delimiter, Address Prefix, and Address Delimiter fields to specify strings for matching the authentication event and for identifying the user mapping information in syslog messages. <p>The remaining fields in the dialog vary based on your selection. Configure the fields for the desired type as described in the following rows.</p>
Event Regex	Enter the regex to match successful authentication events. For the sample message, the regex <code>(authentication) success</code> {1} extracts the first {1} instance of the string <code>authentication success</code> . The backslash before the space is a standard regex escape character that instructs the regex engine not to treat the space as a special character.
Username Regex	Enter the regex to identify the start of the username in authentication success messages. In the sample message, the regex <code>User: ([a-zA-Z0-9\\\\._]+)</code> matches the string <code>User:john Doe_4</code> and extracts <code>domain\john Doe_4</code> as the username.
Address Regex	Enter the regex to identify the IP address portion of authentication success messages. In the sample message, the regular expression <code>Source:([0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3})</code> matches the IPv4 address <code>Source:192.168.0.212</code> and adds <code>192.168.0.212</code> as the IP address in the username mapping.
Event String	Enter a matching string to identify successful authentication events in syslog messages. For the sample message, you would enter the string <code>authentication success</code> .
Username Prefix	Enter a matching string to identify the start of the username field in syslog messages. The field does not support regex expressions such as /s (for a space) or /t (for a tab). In the sample message, <code>User:</code> identifies the start of the username field.

Field	Description
Username Delimiter	Enter the delimiter that indicates the end of the username field in syslog messages. Use \s to indicate a standalone space (as in the sample message) and \t to indicate a tab.
Address Prefix	Enter a matching string to identify the start of the IP address field in syslog messages. The field does not support regex expressions such as /s (for a space) or /t (for a tab). In the sample message, Source: identifies the start of the address field.
Address Delimiter	Enter the delimiter that indicates the end of the IP address field in syslog messages. For example, enter \n to indicate the delimiter is a line break.

Manage the User Ignore List

- ▲ Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > User Ignore List

The ignore user list defines which user accounts don't require IP address-to-username mapping (for example, kiosk accounts). To configure the list, click **Add** and enter a username. You can use an asterisk as a wildcard character to match multiple usernames but only as the last character in the entry. For example, `corpdomain\it-admin*` matches all administrators in the `corpdomain` domain whose usernames start with the string `it-admin`. You can add up to 5,000 entries to exclude from user mapping.

Monitor Servers

- ▲ Device > User Identification > User Mapping

Use the Server Monitoring section to define the Microsoft Exchange Servers, Active Directory (AD) domain controllers, Novell eDirectory servers, or syslog senders that the User-ID agent monitors for login events.

- [Manage Access to Monitored Servers](#)
- [Configure Access to Monitored Servers](#)

Manage Access to Monitored Servers

Perform the following tasks in the Server Monitoring section to manage access to the servers that the User-ID agent monitors for user mapping information.

Task	Description
Display server information	For each monitored server, the User Mapping page displays the Status of the connection from the User-ID agent to the server. After you Add a server, the firewall tries to connect to it. If it succeeds, the Server Monitoring section displays Connected in the Status column. If the firewall cannot connect, the Status column displays an error condition, such as Connection refused or Connection timeout. For details on the other fields that the Server Monitoring section displays, see Configure Access to Monitored Servers .
Add	To Configure Access to Monitored Servers , Add each server that the User-ID agent will monitor for user mapping information.
Delete	To remove a server from the user mapping process (discovery), select the server and Delete it. To remove a server from discovery without deleting its configuration, edit the server entry and clear Enabled . 
Discover	You can automatically Discover Microsoft Active Directory domain controllers using DNS. The firewall will discover domain controllers based on the domain name entered in the Device > Setup > Management page, General Settings section, Domain field. After discovering a domain controller, the firewall creates an entry for it in the Server Monitoring list; you can then enable the server for monitoring.  The Discover feature works for domain controllers only, not Exchange servers or eDirectory servers.

Configure Access to Monitored Servers

Use the Server Monitoring section to **Add** up to 100 servers for the firewall to monitor.



The complete procedure to configure the PAN-OS integrated User-ID agent to monitor servers requires additional tasks.

Server Monitoring Setting	Description
Name	Enter a name for the server.
Description	Enter a description of the server.
Enabled	Select this option to enable log monitoring for this server.
Type	Select the server type. Your selection determines which other fields this dialog displays.
Network Address	If the server Type is Microsoft Active Directory , Microsoft Exchange , or Syslog Sender , enter the server IP address or FQDN.
Server Profile	If the server Type is Novell eDirectory , select an LDAP server profile for connecting to the Novell eDirectory server. For details, see Device > Server Profiles > LDAP .

Server Monitoring Setting	Description
Connection Type	If the server Type is Syslog Sender , select whether the User-ID 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 Enable Server Monitoring settings determines the SSL/TLS versions that are allowed and the certificate that the firewall uses to connect to the syslog sender.
Filter	If the server Type is Syslog Sender , select a Syslog Parse profile to use for extracting usernames and IP addresses from the syslog messages received from this server. You create the profiles when configuring Manage Syslog Message Filters .
Default Domain Name	(Optional) If the server Type is Syslog Sender , enter a domain name to prepend to the username if the log entry has no domain name.

Define Subnetworks to Include/Exclude for User Mapping

▲ Device > User Identification > User Mapping

Use the Include/Exclude Networks list to configure the rules that define which subnetworks the User-ID agent will include or exclude when collecting IP address-to-username mappings. By default, if the list is empty, the User-ID agent collects mappings for user identification sources in all subnetworks using any collection method that you configured. The exception is when using the WMI probing method for client systems that have public IPv4 addresses. (Public IPv4 addresses are those outside the scope of [RFC 1918](#) and [RFC 3927](#)). To enable WMI probing for public IPv4 addresses, you must configure **Include** rules for the subnetworks where those addresses reside.

The User-ID agent applies an implicit exclude all rule to the list. For example, if you add an **Include** rule for subnetwork 10.0.0.0/8, the User-ID agent excludes all other subnetworks even if you don't add **Exclude** rules for them. Add **Exclude** rules only if you want the User-ID agent to exclude a subset of the subnetworks specified in an **Include** rule. For example, if you add an **Exclude** rule for 10.2.48.0/22 and add an **Include** rule for 10.0.0.0/8, the User-ID agent will collect mappings from all the subnetworks of 10.0.0.0/8 except 10.2.48.0/22, and will exclude all subnetworks outside of 10.0.0.0/8. If you add **Exclude** rules without adding any **Include** rules, the User-ID agent excludes all subnetworks, not just the ones you added.

By default, when determining whether to collect user mapping information for a particular user identification source, the User-ID agent evaluates the rules from top to bottom in the order that the Include/Exclude Networks list displays them. The User-ID agent includes or excludes the source based only on the first rule that matches that source to a subnetwork; the agent does not evaluate any subsequent rules. This means you must list the rules from top to bottom in the order of most to least restrictive. For example, because the 10.2.48.0/22 subnetwork is a subset of the 10.0.0.0/8 subnetwork, you would add an **Exclude** rule for

10.2.48.0/22 above an **Include** rule for 10.0.0.0/8 to ensure that the User-ID agent skips mapping collection for any 10.2.48.0/22 sources. If you need to change the evaluation order after adding rules, you can create a **Custom Include/Exclude Network Sequence**.

If you configure the firewall to [redistribute user mapping information](#) to other firewalls, the limits you specify in the Include/Exclude Networks list will apply to the redistributed information.

You can perform the following tasks on the Include/Exclude Networks list:

Task	Description
Add	To limit discovery to a specific subnetwork, Add a subnetwork profile and complete the following fields: <ul style="list-style-type: none">• Name—Enter a name to identify the subnetwork.• Enabled—Select this option to enable inclusion or exclusion of the subnetwork for server monitoring.• Discovery—Select whether the User-ID agent will Include or Exclude the subnetwork.• Network Address—Enter the IP address range of the subnetwork.
Delete	To remove a subnetwork from the list, select and Delete it.  To disable a rule without removing it, edit the rule and clear Enabled .
Custom Include/Exclude Network	By default, the User-ID agent evaluates the rules in the order you add them, from top-first to bottom-last. To change the evaluation order, create a Custom Include/Exclude Network Sequence and then Add, Delete, Move Up, or Move Down the rules as necessary.

Device > User Identification > User-ID Agents

The firewall can receive user mappings from Windows-based User-ID agents or from other firewalls serving as User-ID agents. You must configure access from the firewall to these User-ID agents.



The complete procedures to [configure user mapping using Windows-based User-ID agents](#) and to [configure user mapping redistribution](#) require additional tasks.

- [Manage Access to User-ID Agents](#)
- [Configure Access to User-ID Agents](#)

Manage Access to User-ID Agents

Perform the following tasks for managing connections from the firewall to User-ID agents.

Task	Description
Display information / Refresh Connected	Select the Device > User Identification > User-ID Agents page to see whether the firewall is Connected to each User-ID agent. The Connected column displays a green icon to indicate a successful connection, a yellow icon to indicate a disabled connection, and a red icon to indicate 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. For the other fields that this page displays, see Configure Access to User-ID Agents .
Add	Click Add to Configure Access to User-ID Agents .
Delete	To remove the configuration that enables the firewall to connect to a User-ID agent, select the agent and click Delete .  To disable access to a User-ID agent without deleting its configuration, edit it and clear Enabled .
Custom Agent Sequence	If you enable User-ID agents to perform NT LAN Manager (NTLM) authentication on behalf of the firewall, then by default the firewall communicates with the agents in the order you add them, from top to bottom (see the Use for NTLM Authentication field in Configure Access to User-ID Agents). To change the order, click Custom Agent Sequence , Add each agent, click Move Up or Move Down to reposition the agents, and click OK .

Configure Access to User-ID Agents

To configure the firewall to access a User-ID agent, click **Add** and complete the following fields.

User-ID Agent Setting	Description
Name	<p>Enter a name (up to 31 characters) to identify the User-ID agent. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.</p>  For a firewall serving as a User-ID agent for user mapping redistribution, this field does not have to match the Collector Name field.
Host	<ul style="list-style-type: none"> Windows-based User-ID agent—Enter the IP address of the Windows host on which the User-ID agent is installed. Firewall User-ID agent—Enter the hostname or IP address of the interface (service route) on the firewall that serves as a User-ID agent to redistribute user mappings to the firewall you are logged into. For details on service routes, see Device > Setup > Services.
Port	<p>Enter the port number on which the User-ID agent will listen for User-ID requests. The default is 5007 but you can specify any available port. Different User-ID agents can use different ports.</p>  Some earlier versions of the User-ID agent use 2010 as the default port.
Collector Name	These fields apply only if the User-ID agent is another firewall that redistributes user mappings to the firewall you are logged into. Enter the Collector Name and Pre-Shared Key that are configured on the User-ID agent (see Enable Redistribution of User Mappings Among Firewalls). The firewall you are logged into uses the key to establish an SSL connection with the User-ID agent.
Collector Pre-shared Key/Confirm Collector Pre-shared key	
Use as LDAP Proxy	<p>Select this option if you want the firewall to use this User-ID agent as a proxy for collecting group mapping information from a directory server. To use this option, you must also configure group mapping on the firewall (see Device > User Identification > Group Mapping Settings). The firewall pushes that configuration to the User-ID agent to enable it to collect the mapping information.</p> <p>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 having to query the server directly.</p>
Use for NTLM Authentication	<p>Select this option if you want the firewall to use this User-ID agent as a proxy for performing NT LAN Manager (NTLM) authentication when a client web request matches a Captive Portal rule. The User-ID agent collects user mapping information from the domain controller and forwards it to the firewall. To use this option, you must also Enable NTLM Authentication on the User-ID agent.</p> <p>This option is useful in deployments where the firewall cannot directly access the domain controller to perform NTLM authentication. It is also useful in deployments that benefit from reducing the number of authentication requests the domain controller must process; multiple firewalls can receive the user mapping information from the cache on a single User-ID agent instead of each firewall directly querying the domain controller.</p>
Enabled	Select this option to enable the firewall to communicate with the User-ID agent.

Device > User Identification > Terminal Services Agents

On a system that support multiple users who share the same IP address, a Terminal Services (TS) agent identifies individual users by allocating port ranges to each one. The TS agent notifies every connected firewall about the allocated port range so that the firewalls can enforce policy based on users and user groups. You can perform the following tasks to manage access to TS agents.



You must install and configure the TS agents before configuring access to them. The [complete procedure](#) to configure user mapping for terminal server users requires additional tasks.

Task	Description
Display information / Refresh Connected	In the Terminal Services Agents page, the Connected column displays the status of the connections from the firewall to the TS agents. A green icon indicates a successful connection, a yellow icon indicates a disabled connection, and a red icon indicates a failed connection. If you think the connection status might have changed since you first opened the page, click Refresh Connected to update the status display.
Add	To configure access to a TS agent, click Add and complete the following fields: <ul style="list-style-type: none">• 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 where the TS agent is installed.• Port—Enter the port number (default is 5009) that the TS agent service will use to communicate with the firewall.• 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 enter up to eight additional IP addresses.• Enabled—Select this option to enable the firewall to communicate with this TS agent.
Delete	To remove the configuration that enables access to a TS agent, select the agent and click Delete . To disable access to a TS agent without deleting its configuration, edit the agent and clear Enabled .

Device > User Identification > Group Mapping Settings

To base security policies on user or group, the firewall must retrieve the list of groups and the corresponding list of members from your directory servers. The firewall supports a variety of LDAP directory servers, including Microsoft Active Directory (AD), Novell eDirectory, and Sun ONE Directory Server.



Before creating a group mapping configuration, you must configure an LDAP server profile (see [Device > Server Profiles > LDAP](#)). The [complete procedure](#) to map usernames to groups requires additional tasks.

Add a group mapping configuration for each LDAP server in your network. To remove a group mapping configuration, select it and click **Delete**. If you want to disable a group mapping configuration without deleting it, edit the configuration and clear the **Enabled** selection. When adding a group mapping configuration, complete the following fields.

Group Mapping Setting—Server Profile	Configured In	Description
Name	Device > User Identification > Group Mapping Settings	Enter a name to identify the group mapping configuration (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Server Profile	Device > User Identification > Group Mapping Settings > Server Profile	Select the LDAP server profile to use for group mapping on this firewall.
Update Interval		Specify the interval in seconds after which the firewall will initiate a connection with the LDAP directory server to obtain any updates that were made to the groups that firewall policies use (range is 60–86400).
User Domain		<p>By default, the User Domain field is blank and the firewall automatically detects the domain names for Active Directory servers. If you enter a value, it overrides any domain names that the firewall retrieves from the LDAP source. Your entry must be the NetBIOS name.</p> <p> 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 Device > Authentication Profile).</p>

Group Mapping Setting—Server Profile	Configured In	Description
Group Objects		<ul style="list-style-type: none"> Search Filter—Enter an LDAP query that specifies which groups to retrieve and track. Object Class—Enter a group definition. The default is objectClass=group, which specifies that the system retrieves all objects in the directory that match the group Search Filter and have objectClass=group. Group Name—Enter the attribute that specifies the group name. For example, in Active Directory, this attribute is “CN” (Common Name). Group Member—Enter the attribute that contains the group members. For example in Active Directory, this attribute is “member.”
User Objects		<ul style="list-style-type: none"> Search Filter—Enter an LDAP query that specifies which users to retrieve and track. Object Class—Enter a user object definition. For example in Active Directory, the objectClass is “user.” User Name—Enter the attribute for the username. For example, in Active Directory, the default username attribute is “samAccountName.”
Mail Domains		<p>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 contains a link to the user that, when clicked, displays the ACC filtered by the user. If the email is sent to a distribution list, the ACC is filtered by the members contained in the list.</p> <p>The email header and user mapping information will help you quickly track and thwart threats that arrive through email by making it easier to identify the users who received the email.</p> <ul style="list-style-type: none"> Mail Attributes—PAN-OS automatically populates this field based on the LDAP server type (Sun ONE, Active Directory, or Novell). Domain List—Enter the email domains in your organization as a comma separated list of up to 256 characters.
Enabled		Select this option to enable server profile for group mapping.

Group Mapping Setting—Server Profile	Configured In	Description
Available Groups	Device > User Identification > Group Mapping Settings > Group Include List	<p>Use these fields to limit the number of groups that the firewall displays when you create a security rule. Browse the LDAP tree to find the groups you want to use in rules. To include a group, select it in the Available Groups list and Add () it. To remove a group from the list, select it in the Included Groups list and Delete () it.</p> <p>The maximum number of groups you can add in the Group Include List tab and Custom Group tab combined is 640 per virtual system.</p>
Name	Device > User Identification > Group Mapping Settings > Custom Group	<p>Use these fields 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 the LDAP directory. The User-ID service maps all the LDAP directory users who match the filter to the custom group. If you create a custom group with the same Distinguished Name (DN) as an existing Active Directory group domain name, the firewall uses the custom group in all references to that name (for example, in policies and logs). To create a custom group, click Add and configure the following fields:</p> <ul style="list-style-type: none"> • Name—Enter a custom group name that is unique in the group mapping configuration for the current firewall or virtual system. • LDAP Filter—Enter a filter of up to 2,048 characters. 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. The firewall does not validate LDAP filters. <p>To delete a custom group, select it and click Delete. To make a copy of a custom group, select it, click Clone and edit the fields as necessary.</p> <p>The maximum number of groups you can add in the Group Include List tab and Custom Group tab combined is 640 per virtual system.</p> <p> After creating or cloning a custom group, you must perform a commit for it to be available in policies and objects.</p>
LDAP Filter		

Device > User Identification > Captive Portal Settings

In the **Device > User Identification > Captive Portal Settings** page, Edit () the following settings to configure the firewall to use **Captive Portal authentication**  for user mapping.



If Captive Portal will use an SSL/TLS Service Profile (see [Device > Certificate Management > SSL/TLS Service Profile](#)), authentication profile (see [Device > Authentication Profile](#)), or Certificate Profile (see [Device > Certificate Management > Certificate Profile](#)), configure the profile before starting. The [complete procedure](#)  to configure Captive Portal for user mapping requires additional tasks.

Field	Description
Enable Captive Portal	Select this option to enable the Captive Portal option for user identification.
Idle Timer (min)	Enter the user time to live (user TTL) in minutes for a Captive Portal session (range is 1-1440; default is 15). This timer resets every time there is activity from a Captive Portal user. If the time the user is idle exceeds the Idle Timer value, PAN-OS removes the Captive Portal user mapping and the user must log in again.
Timer (min)	This is the maximum TTL in minutes, which is the maximum time that any Captive Portal session can remain mapped (range is 1-1440; default is 60). After this duration elapses, PAN-OS removes the mapping and users must re-authenticate even if the session is active. This timer prevents stale mappings and the value set here overrides the Idle Timer value. Therefore, the best practice is to set the expiration Timer higher than the Idle Timer .
SSL/TLS Service Profile	To specify a firewall server certificate and the allowed protocols for securing redirect requests, select an SSL/TLS service profile (see Device > Certificate Management > SSL/TLS Service Profile). If you select None , the firewall will use its 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 web requests.
Authentication Profile	Select an authentication profile for authenticating users who are redirected to a web form for authentication (see Device > Authentication Profile). Even if Captive Portal will use Kerberos single sign-on (SSO) or NT LAN Manager (NTLM) authentication, you must assign an Authentication Profile or Certificate Profile to authenticate users in case Kerberos SSO or NTLM authentication fails or the client or browser does not support it.

Field	Description
Mode	<p>Select how the firewall captures web requests for authentication:</p> <ul style="list-style-type: none"> • Transparent—The firewall intercepts browser traffic according to the Captive Portal rule and impersonates the original destination URL, issuing an HTTP 401 to prompt the user to authenticate. However, because the firewall does not have the real certificate for the destination URL, the browser displays a certificate error to users attempting to access a secure site. Therefore, only use this mode when absolutely necessary, such as in Layer 2 or virtual wire deployments. • Redirect—The firewall intercepts unknown HTTP or HTTPS sessions and redirects them to a Layer 3 interface on the firewall using an HTTP 302 redirect to prompt the user to authenticate. This is the preferred mode because it provides a better end-user experience (no certificate errors). However, it requires that you enable response pages on the Interface Management profile assigned to the Layer 3 interface to which the firewall redirects web requests (for details, see Network > Network Profiles > Interface Mgmt and Layer 3 Interface). Another benefit of the Redirect mode is that it allows for session cookies, which enable the user to continue browsing to authenticated sites without requiring re-mapping each time the timeouts expire. This is especially useful for users who roam from one IP address to another (for example, from the corporate LAN to the wireless network) because they won't need to re-authenticate upon changing IP address as long as the session stays open. If Captive Portal will use Kerberos SSO (recommended) or NTLM authentication, Redirect mode is required because the browser will only provide credentials to trusted sites.
Session Cookie (Redirect mode only)	<ul style="list-style-type: none"> • Enable—Select this option to enable session cookies. • Timeout—If you Enable session cookies, this timer specifies the number of minutes for which the cookie is valid (range is 60-10080; default is 1440). • Roaming—Select this option to retain the cookie if the IP address changes while the session is active (for example, if the client moves from a wired to a wireless network). The user must re-authenticate only if the cookie times out or the user closes the browser.
Redirect Host (Redirect mode only)	<p>Specify the intranet hostname that resolves to the IP address of the Layer 3 interface to which the firewall redirects web requests.</p> <p> If users authenticate through Kerberos single sign-on (SSO), the Redirect Host must be the same as the hostname specified in the Kerberos keytab.</p>
Certificate Profile	<p>Select a Certificate Profile for authenticating Captive Portal users (see Device > Certificate Management > Certificate Profile). For this authentication type, Captive Portal prompts the browser to present a valid client certificate to authenticate the user. For this method, you must deploy client certificates on each user system. Furthermore, on the firewall, you must install the trusted certificate authority (CA) certificate used to issue the client certificates and assign the CA certificate to the certificate profile. This is the only authentication method that enables Transparent authentication for Mac OS and Linux clients.</p>

Field	Description
NTLM Authentication	<p>When you configure Captive Portal for NT LAN Manager (NTLM) authentication, the firewall uses an encrypted challenge-response mechanism to obtain user credentials from the browser. When configured properly, the browser provides 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 Certificate Profile authentication, depending on how you configure Captive Portal. By default, Internet Explorer supports NTLM. You can configure Firefox and Chrome to use it. You cannot use NTLM to authenticate non-Windows clients.</p>  These options apply only to the Windows-based User-ID agents. When using the PAN-OS integrated User-ID agent, the firewall must be able to successfully resolve the DNS name of your domain controller to join the domain. You can then enable Enable NTLM Authentication in the PAN-OS integrated User-ID agent setup and provide the credentials for the firewall to join the domain. NTLM is available only for Windows Server version 2003 and earlier versions.

To configure NTLM for use with Windows-based User-ID agents, define the following:

- **Attempts**—The number of attempts after which NTLM authentication fails (range is 1-60; default is 1).
- **Timeout**—The number of seconds after which NTLM authentication times out (range is 1-60; default is 2).
- **Reversion Time**—The number of seconds after which the firewall will retry contacting the first User-ID agent listed in the [Device > User Identification > User-ID Agents](#) page after that agent becomes unavailable (range is 60-3600; default is 300).



As a best practice, choose [Kerberos SSO](#) transparent authentication over NTLM authentication when configuring Captive Portal. Kerberos is a stronger, more robust authentication method than NTLM and it does not require the firewall to have an administrative account to join the domain.



GlobalProtect

GlobalProtect provides a complete infrastructure for managing your mobile workforce to enable secure access for all of your users, regardless of what devices they are using or where they are located. The following firewall web interface pages allow you to configure and manage GlobalProtect components:

- ▲ [Network > GlobalProtect > Portals](#)
- ▲ [Network > GlobalProtect > Gateways](#)
- ▲ [Network > GlobalProtect > MDM](#)
- ▲ [Network > GlobalProtect > Block List](#)
- ▲ [Objects > GlobalProtect > HIP Objects](#)
- ▲ [Objects > GlobalProtect > HIP Profiles](#)
- ▲ [Device > GlobalProtect Client](#)

Looking for more?

See the [GlobalProtect Administrator's Guide](#) to learn more about GlobalProtect, including details on setting up the GlobalProtect infrastructure, how to use host information to enforce policy, and step-by-step instructions for configuring common GlobalProtect deployments.

Network > GlobalProtect > Portals

Select **Network > GlobalProtect > Portals** to set up and manage a GlobalProtect™ portal. The portal provides the management functions for the GlobalProtect infrastructure. Every client system that participates in the GlobalProtect network receives its configuration from the portal, including information about the available gateways and any client certificates that might be necessary for the client to connect to a gateway. In addition, the portal controls the behavior and distribution of the GlobalProtect agent software to Mac and Windows laptops. (For mobile devices, the GlobalProtect app is distributed through the web store for that device—Apple App Store for iOS devices, Google Play for Android devices, Microsoft Store for Windows 10 phone and other Windows 10 UWP devices, and, for Chromebooks, the GlobalProtect app is distributed by the Chromebook Management Console or through Google Play).

To add a portal configuration, click **Add** to open the GlobalProtect Portal dialog.

What do you want to know?	See:
What general settings should I configure for the GlobalProtect portal?	GlobalProtect Portals General Tab
How can I assign an authentication profile to a portal configuration?	GlobalProtect Portals Authentication Configuration Tab
What client authentication options can I configure?	GlobalProtect Portals Agent Authentication Tab
How can I assign a configuration to a specific group of devices based on operating system, user, and/or user group?	GlobalProtect Portals Agent User/User Group Tab
How can I configure the settings and priority of the internal and external gateways?	GlobalProtect Portals Agent Gateways Tab
How can I create separate client configurations for different types of users?	GlobalProtect Portals Agent Configuration Tab
What settings can I customize on the look and behavior of the GlobalProtect agent?	GlobalProtect Portals Agent App Tab
How can I configure data collection options?	GlobalProtect Portals Agent Data Collection Tab
How can I extend VPN connectivity to a firewall which acts as a satellite?	GlobalProtect Portals Satellite Configuration Tab
Looking for more?	For detailed, step-by-step instructions on setting up the portal, refer to Configure a GlobalProtect Portal in the <i>GlobalProtect Administrator's Guide</i> .

GlobalProtect Portals General Tab

Select **Network > GlobalProtect > Portals > <GlobalProtect-portal-config> > General** to define the network settings that an agent or app uses to connect to the GlobalProtect portal. Optionally, you can disable the login page or specify a custom portal login and help pages for GlobalProtect. For information on how to create and import custom pages, refer to [Customize the Portal Login, Welcome, and Help Pages](#) in the [GlobalProtect Administrator's Guide](#).

GlobalProtect Portal Setting	Description
Name	Type a name for the portal (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in multiple virtual system mode, the Location is the virtual system (vsys) where the GlobalProtect portal is available. For a firewall that is not in multi-vsys mode, Location selection is not available. After you save the portal, you cannot change Location .
Network Settings	
Interface	Select the name of the firewall interface that will be the ingress for communications from remote clients and firewalls.
IP Address	Specify the IP address on which the GlobalProtect portal web service is to run.
Appearance	
Disable login page	Select this option to disable access to the GlobalProtect portal login page from a web browser.
Custom Login Page	(Optional) Choose a custom login page for user access to the portal.
Custom Help Page	(Optional) Choose a custom help page to assist the user with GlobalProtect.

GlobalProtect Portals Authentication Configuration Tab

Select **Network > GlobalProtect > Portals > <GlobalProtect-portal-config> > Authentication** to configure several different types of GlobalProtect portal settings:

- An SSL/TLS service profile that the portal and servers use for authentication. The service profile is independent of the other settings in Authentication.
- Unique authentication schemes that are based primarily on the operating system of the user endpoints and secondarily on an optional authentication profile.
- **(Optional) A Certificate Profile**, which enables GlobalProtect to use a specific certificate profile for authenticating the user. The certificate from the client must match the certificate profile (if client certificates are part of the security scheme).

GlobalProtect Portal Authentication Setting	Description
Server Authentication	
SSL/TLS Service Profile	<p>Select an existing SSL/TLS Service profile. The profile specifies a certificate and the allowed protocols for securing traffic on the management interface. The Common Name (CN) and, if applicable, the Subject Alternative Name (SAN) fields of the certificate associated with the profile must match the IP address or fully qualified domain name (FQDN) of the Interface selected in the General tab.</p> <p>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.</p>
Client Authentication	
Name	<p>Enter a name to identify the client authentication configuration. (The client authentication configuration is independent of the SSL/TLS service profile.). You can create multiple client authentication configurations and differentiate them primarily by operating system and additionally by unique authentication profiles (for the same OS). For example, you can add client authentication configurations for different operating systems but also have different configurations for the same OS that are differentiated by unique authentication profiles. (You should manually order these profiles from most specific to most general. For example, all users and any OS is the most general.)</p> <p>You can also create configurations that GlobalProtect deploys to agents in pre-logon mode (before the user has logged in to the system) or that it applies to any user. (Pre-logon establishes a VPN tunnel to a GlobalProtect gateway before the user logs in to GlobalProtect.)</p>
OS	<p>To deploy a client authentication profile specific to the operating system (OS) on an endpoint, Add the OS (Android, Chrome, iOS, Mac, Windows, or WindowsUWP). The OS is the primary differentiator between configurations. (See Authentication Profile for further differentiation.)</p> <p>The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite (LSVPN).</p>

GlobalProtect Portal Authentication Setting	Description
Authentication Profile	<p>In addition to distinguishing a client authentication configuration by an OS, you can further differentiate by specifying an authentication profile. (You can create a New Authentication Profile or select an existing one.) To configure multiple authentication options for an OS, you can create multiple client authentication profiles.</p>  <p>If you are configuring an LVPN in Gateways, you cannot save that configuration unless you select an authentication profile here. Also, if you plan to use serial numbers to authenticate satellites, the portal must have an authentication profile available when it cannot locate or validate a firewall serial number.</p> <p>Refer also to Device > Authentication Profile.</p>
Authentication Message	To help end users know the type of credentials they need for logging in, enter a message or keep the default message. The maximum length of the message is 100 characters.
Certificate Profile	
Certificate Profile	<p>(Optional) Select the Certificate Profile the portal uses to match those client certificates that come from user endpoints. With a Certificate Profile, the portal authenticates the user only if the certificate from the client matches this profile.</p> <p>The certificate profile is independent of the OS. Also, this profile is active even if you enable Authentication Override, which overrides the Authentication Profile to allow authentication using encrypted cookies.</p>

GlobalProtect Portals Agent Configuration Tab

Select **Network > GlobalProtect > Portals > <GlobalProtect-portal-config> > Agent** to define the agent configuration settings. The GlobalProtect portal deploys the configuration to the device after the connection is first established.

You can also specify that the portal automatically deploy trusted root certificate authority (CA) certificates and intermediate certificates. If the endpoints do not trust the server certificates that the GlobalProtect gateways and GlobalProtect Mobile Security Manager are using, the endpoints need these certificates to establish HTTPS connections to the gateways or Mobile Security Manager. The portal pushes the certificates you specify here to the client along with the client configuration.

To add a trusted root CA certificate, **Add** an existing certificate or **Import** a new one. To install (transparently) the trusted root CA certificates that are required for SSL Forward Proxy decryption in the certificate store on the client, select **Install in Local Root Certificate Store**.

If you have different types of users that require different configurations, you can create separate agent configurations to support them. The portal subsequently uses the user or group name and OS of the client to determine the agent configuration to deploy. As with security rule evaluations, the portal looks for a match, starting from the top of the list. When the portal finds a match, it delivers the corresponding configuration to the agent/app. Therefore, if you have multiple agent configurations, it is important to order them so that more specific configurations (such as those for specific users or operating systems) are above the more generic configurations. Use **Move Up** and **Move Down** to reorder the configurations. As needed, **Add** a new agent configuration. For detailed information on configuring the portal and creating agent

configurations, refer to [Configure the GlobalProtect Portal](#) in the [GlobalProtect Administrator's Guide](#). When you **Add** a new agent configuration or modify an existing one, the agent Configs dialog opens and displays five tabs, which are described in the following tables:

- [GlobalProtect Portals Agent Authentication Tab](#)
- [GlobalProtect Portals Agent User/User Group Tab](#)
- [GlobalProtect Portals Agent Gateways Tab](#)
- [GlobalProtect Portals Agent App Tab](#)
- [GlobalProtect Portals Agent Data Collection Tab](#)

GlobalProtect Portals Agent Authentication Tab

Select **Network > GlobalProtect > Portals > <GlobalProtect-portal-config> > Agent > <agent-config> > Authentication** to configure the authentication settings that apply to the agent configuration.

GlobalProtect Portal Client Authentication Configuration Setting	Description
Authentication Tab	
Name	Enter a descriptive name for this configuration for client authentication.
Client Certificate	<p>(Optional) Select the source that distributes the client certificate to a client, which then presents the certificate to the gateways. A client certificate is required if you are configuring mutual SSL authentication.</p> <p>If SCEP is configured for pre-logon in the portal client configuration, the portal generates a machine certificate that is stored in the system certificate store for gateway authentication and connections.</p> <p>To use a certificate that is Local to the firewall instead of a generated certificate from the PKI through SCEP, select a certificate that is already uploaded to the firewall.</p> <p>If you use an internal CA to distribute certificates to clients, select None (default). When you select None, the portal does not push a certificate to the client.</p>
Save User Credentials	Select Yes to save the username and password on the agent or select No to force the users to provide the password—either transparently via the client or by manually entering one—each time they connect. Select Save Username Only to save only the username each time a user connects.
Authentication Override	
Generate cookie for authentication override	Select this option to configure the portal to generate encrypted, endpoint-specific cookies. The portal sends this cookie to the endpoint after the user first authenticates with the portal.
Cookie Lifetime	Specify the hours, days, or weeks that the cookie is valid. The typical lifetime is 24 hours. The ranges are 1–72 hours, 1–52 weeks, or 1–365 days. After the cookie expires, the user must enter login credentials and the portal subsequently encrypts a new cookie to send to the user endpoint.

GlobalProtect Portal Client Authentication Configuration Setting	Description
Accept cookie for authentication override	Select this option to configure the portal to authenticate clients through a valid, encrypted cookie. When the endpoint presents a valid cookie, the portal verifies that the cookie was encrypted by the portal, decrypts the cookie, and then authenticates the user.
Certificate to Encrypt/Decrypt Cookie	<p>Select the certificate to use for encrypting and decrypting the cookie.</p>  Ensure that the portal and gateways use the same certificate to encrypt and decrypt cookies. (Configure the certificate as part of a gateway client configuration. See Network > GlobalProtect > Gateways).
Two-Factor Authentication	
<p>To configure GlobalProtect to support dynamic passwords—such as one-time passwords (OTPs)—specify the portal or gateway types that require users to enter dynamic passwords. Where two-factor authentication is not enabled, GlobalProtect uses regular authentication using login credentials (such as AD) and a certificate.</p> <p>When you enable a portal or a gateway type for two-factor authentication, that portal or gateway prompts the user after initial portal authentication to submit credentials and a second OTP (or other dynamic password). However, if you also enable authentication override, an encrypted cookie is used to authenticate the user (after the user is first authenticated for a new session) and, thus, preempts the requirement for the user to re-enter credentials (as long as the cookie is valid). Therefore, the user is transparently logged in whenever necessary as long as the cookie is valid. You specify the lifetime of the cookie.</p>	
Portal authentication	Select this option to use dynamic passwords to connect to the portal.
Internal gateway authentication	Select this option to use dynamic passwords to connect to internal gateways.
Manual only external gateway authentication	Select this option to use dynamic passwords to connect to external gateways that are configured as Manual gateways.
Auto discovery external gateway authentication	Select this option to use dynamic passwords to connect to any remaining external gateways that the agent can automatically discover (gateways which are not configured as Manual).

GlobalProtect Portals Agent User/User Group Tab

Select **Network > GlobalProtect > Portals > <GlobalProtect-portal-config> > Agent > <agent-config> > User/User Group** to specify the operating systems and users or user groups to which this agent configuration applies. If this agent configuration cannot accommodate all combinations of operating systems and users capabilities, consider adding another agent configuration. If you have multiple agent configurations that are differentiated by operating systems and users or user groups, the most specific configurations should be at the top of the table in Agent and the most general (such as any OS and a broad group membership) at the bottom. You can move an agent configuration up or down as needed.

For groups, the only supported type of authentication service is LDAP.

GlobalProtect Portal Client User/User Group Configuration Setting	Description
OS	<p>A user or group member can have multiple devices whose operating systems differ from each other (for example, a user with one endpoint running Windows OS and another endpoint running Mac OS). The portal can provide configurations that are specific to the OS on each endpoint. For the current agent configuration, you can Add one or more client operating systems to specify which clients receive the configuration. A portal automatically learns the OS of the client device and incorporates details for that OS in the client configuration. You can select Any OS or a specific OS (Android, Chrome, iOS, Mac, Windows, or WindowsUWP); you can also select more than one OS. The information in User/User Groups describes how you can further differentiate by selection of users, user groups, and choice of any, pre-logon or select.</p>
User/User Group	<p>You can Add individual users or user groups to which the current agent configuration applies.</p> <p> You must configure group mapping (Device > User Identification > Group Mapping Settings) before you can select the groups.</p> <p>In addition to users and groups, you can use the drop-down to specify when these settings apply to the users or groups:</p> <ul style="list-style-type: none"> • any—The agent configuration applies to all users (no need to Add users or user groups). • select—The agent configuration applies only to users and user groups you Add to this list. • pre-logon—The agent configuration applies only to the users and user groups you Add that also are configured for pre-logon or pre-logon then on-demand. To use the pre-logon option, you must also enable a pre-logon (or pre-logon then on-demand) Connect Method in the App tab for this agent configuration.

GlobalProtect Portals Agent Gateways Tab

Select **Network > GlobalProtect > Portals > <GlobalProtect-portal-config> > Agent > <agent-config> > Gateways** to configure the settings for internal and external gateways for an agent configuration.

GlobalProtect Portal Gateway Setting	Description
Internal Gateways	
Specify the internal firewalls to which an agent or app can request access and also provide HIP reports (if HIP is enabled in the GlobalProtect Portals Agent Data Collection Tab).	<p>Add internal gateways that include the following information for each:</p> <ul style="list-style-type: none"> • Name—A label of up to 31 characters to identify the gateway. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. • Address—The IP address or FQDN of the firewall interface for the gateway. This value must match the Common Name (CN) and SAN (if specified) in the gateway server certificate. For example, if you used an FQDN to generate the certificate, you must enter the FQDN here.
External Gateways	
Cutoff Time (sec)	Specify the number of seconds that an agent or app waits for all of the available gateways to respond before it selects the best gateway. For subsequent connection requests, the agent or app tries to connect to only those gateways that responded before the cutoff. A value of 0 means the agent or app uses the TCP timeout—AppConfigurations in the App tab (range is 0-10; default is 5).
Specify the list of firewalls to which agents can try to connect when establishing a tunnel while not on the corporate network.	<p>Add external gateways that include the following information for each:</p> <ul style="list-style-type: none"> • 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 use. The agent will contact all specified 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 option to let users manually select (or switch to) a gateway. The GlobalProtect agent can connect to any external gateway that is configured as Manual. When the agent or app connects to another gateway, the existing tunnel is disconnected and a new tunnel established. The manual gateways can also have a different authentication mechanism than the primary gateway. If a client system is restarted or if a rediscovery is performed, the GlobalProtect agent connects to the primary gateway. This feature is useful if a group of users needs to connect temporarily to a specific gateway to access a secure segment of your network.

GlobalProtect Portal Gateway Setting	Description
Internal Host Detection	
Internal Host Detection	<p>Select this option to allow the GlobalProtect agent to determine if it is inside the enterprise network. This option applies only to endpoints that are configured to communicate with internal gateways.</p> <p>When the user attempts to log in, the agent does a reverse DNS lookup of an internal host using the specified Hostname to the specified IP Address. The host serves as a reference point that is reachable if the endpoint is inside the enterprise network. If the agent finds the host, the endpoint is inside the network and the agent connects to an internal gateway; if the agent fails to find the internal host, the endpoint is outside the network and the agent establishes a tunnel to one of the external gateways.</p>
IP Address	Enter an internal IP Address for internal host detection.
Hostname	Enter the Hostname that resolves to the IP address within the internal network.
Third Party VPN	
Third Party VPN	To direct the GlobalProtect agent or app to ignore selected, third-party VPN clients so that GlobalProtect does not conflict with them, Add the name of the VPN client by selecting the name from the list or entering the name in the field provided. GlobalProtect ignores the route settings for the specified VPN clients if you configure this feature.

GlobalProtect Portals Agent App Tab

Select **Network > GlobalProtect > Portals > <GlobalProtect-portal-config> > Agent > <agent-config> > App** to specify how end users interact with the GlobalProtect agents installed on their systems. You can define different app settings for the different GlobalProtect agent configurations you create.

GlobalProtect App Configuration Setting	Description
Welcome Page	Select a welcome page to present to end users after they connect to GlobalProtect. You can select the factory-default page or Import a custom page. The default is None .
App Configurations	
Connect Method	<ul style="list-style-type: none"> On-demand (Manual user initiated connection)—Users must launch the GlobalProtect agent or app and then initiate a connection to the portal and enter their GlobalProtect credentials. This option is used primarily for remote access connections. User-logon (Always On)—The GlobalProtect agent or app automatically establishes a connection to the portal after the user logs in to an endpoint. The portal responds by providing the client with the appropriate agent configuration. Subsequently, the agent sets up a tunnel to one of the gateways specified in the agent configuration received from the portal. Pre-logon—Pre-logon ensures remote Windows and Mac users are always connected to the corporate network and enables user logon scripts and application of domain policies when the user logs in to the endpoint. Because the endpoint can connect to the corporate network as if it were internal, users can log in with new passwords when their passwords expire or receive help with password recovery if they forget their password. With pre-logon, the GlobalProtect agent establishes a VPN tunnel to a GlobalProtect gateway before the user logs in to the endpoint; the endpoint requests authentication by submitting a pre-installed machine certificate to the gateway. Then, on Windows endpoints, the gateway reassigns the VPN tunnel from the pre-logon user to the username that logged in to the endpoint; on Mac endpoints, the agent disconnects and creates a new VPN tunnel for the user. There are two pre-logon connect methods, either of which enables the same pre-logon functionality that takes place before users log in to the endpoint. However, after users log in to the endpoint, the pre-logon connect method determines when the GlobalProtect agent connection is established: <ul style="list-style-type: none"> Pre-logon (Always On)—The GlobalProtect agent automatically attempts to connect and reconnect to GlobalProtect gateways. Mobile devices do not support pre-logon functionality, and therefore will default to the User-logon (Always On) connect method if this connect method is specified. Pre-logon then On-demand (available only with content release 590-3397 and later releases)—Users must launch the GlobalProtect agent or app and then initiate the connection manually. Mobile devices do not support pre-logon functionality, and therefore will default to the On-demand (Manual user initiated connection) connect method if this connect method is specified.

GlobalProtect App Configuration Setting	Description
GlobalProtect App Config Refresh Interval (hours)	Specify the number of hours the GlobalProtect portal waits before it initiates the next refresh of a client's configuration (range is 1-168; default is 24).
Allow User to Disable GlobalProtect App	<p>Specifies whether users are allowed to disable the GlobalProtect agent and, if so, what—if anything—they must do before they can disable the agent:</p> <ul style="list-style-type: none"> • Allow—Allow any user to disable the GlobalProtect agent as needed. • Disallow—Do not allow end users to disable the GlobalProtect agent. • Allow with Comment—Allow users to disable the GlobalProtect agent or app on their endpoint but require that they submit their reason for disabling the agent. • Allow with Passcode—Allow users to enter a passcode to disable the GlobalProtect agent or app. This option requires the user to enter and confirm a Passcode value that, like a password, does not display when typed. Typically, administrators provide a passcode to users before unplanned or unanticipated events prevent users from connecting to the network by using the GlobalProtect VPN. You can provide the passcode through email or as a posting on your organization's website. • Allow with Ticket—This option enables a challenge-response mechanism where, after a user attempts to disable GlobalProtect, the endpoint displays an 8-character, hexadecimal, ticket request number. The user then contacts the firewall administrator or support team (preferably by phone for security) and provides this number. The administrator or support person types the hexadecimal ticket request number into the Agent User Override Key field (in the GlobalProtect agent configuration Agent tab) so they can see the ticket number (also an 8-character hexadecimal number). The administrator or support person then provides this ticket number to the user who then enters the ticket number into the challenge field to disable the agent.
Allow User to Upgrade GlobalProtect App	<p>Specifies whether end users can upgrade the GlobalProtect agent software and, if they can, whether they can choose when to upgrade:</p> <ul style="list-style-type: none"> • Disallow—Prevent users from upgrading the agent or app software. • Allow Manually—Allow users to manually check for and initiate upgrades by selecting Check Version in the GlobalProtect agent. • Allow with Prompt (default)—Prompt users when a new version is activated on the firewall and allow users to upgrade their software when it is convenient. • Allow Transparently—Automatically upgrade the agent software whenever a new version becomes available on the portal.
Use Single Sign-on (Windows Only)	Select No to disable single sign-on (SSO). With SSO enabled (default), the GlobalProtect agent automatically uses the Windows login credentials to authenticate and then connect to the GlobalProtect portal and gateway. GlobalProtect can also wrap third-party credentials to ensure that Windows users can authenticate and connect even when a third-party credential provider is used to wrap the Windows login credentials.
Clear Single Sign-On Credentials on Logout (Windows Only)	Select No to keep single sign-on credentials when the user logs out. Select Yes (default) to clear them and force the user to enter credentials upon the next login.

GlobalProtect App Configuration Setting	Description
Use Default Authentication on Kerberos Authentication Failure (Windows Only)	Select No to use only Kerberos authentication. Select Yes (default) to retry authentication by using the default authentication method after a failure to authenticate with Kerberos.
Enforce GlobalProtect Connection for Network Access	Select Yes to force all network traffic to traverse a GlobalProtect tunnel. By default, this option is set to No meaning GlobalProtect is not required for network access meaning users can still access the internet if GlobalProtect is disabled or disconnected. To provide instructions to users before traffic is blocked, configure a Traffic Blocking Notification Message and optionally specify when to display the message (Traffic Blocking Notification Delay). To permit traffic required to establish a connection with a captive portal, specify a Captive Portal Exception Timeout . The user must authenticate with the portal before the timeout expires. To provide additional instructions, configure a Captive Portal Detection Message .
Captive Portal Exception Timeout (sec)	To enforce GlobalProtect for network access but provide a grace period to allow users enough time to connect to a captive portal, specify the timeout in seconds (range is 0 to 3600). For example, a value of 60 means the user must log in to the captive portal within one minute after GlobalProtect detects the captive portal. A value of 0 means GlobalProtect does not allow users to connect to a captive portal and immediately blocks access.
Traffic Blocking Notification Delay (sec)	Specify a value, in seconds, to determine when to display the notification message. GlobalProtect starts the countdown to display the notification after the network is reachable (default is 15; range is 5 to 120).
Display Traffic Blocking Notification Message	Specify whether a message appears when GlobalProtect is required for network access. Select No to disable the message. By default the value is set to Yes meaning GlobalProtect displays the message when GlobalProtect is disconnected but detects that network is reachable.
Traffic Blocking Notification Message	Customize a notification message to display to users when GlobalProtect is required for network access. The message can indicate the reason for blocking the traffic and provide instructions on how to connect (for example, To access the network, you must first connect to GlobalProtect.). The message must be 512 or fewer characters.
Allow User to Dismiss Traffic Blocking Notifications	Select No to always display traffic blocking notifications. By default the value is set to Yes meaning users are permitted to dismiss the notifications.
Display Captive Portal Detection Message	Specifies whether a message appears when GlobalProtect detects a captive portal. Select Yes to enable the message. By default the value is set to No meaning GlobalProtect displays the message when GlobalProtect detects a captive portal.
Captive Portal Detection Message	Customize a notification message to display to users when GlobalProtect detects a captive portal. The message can provide additional information about connecting to the captive portal (for example, GlobalProtect has temporarily permitted network access for you to connect to the internet. Follow instructions from your internet provider. If you let the connection time out, open GlobalProtect and click Connect to try again.). The message must be 512 or fewer characters.

GlobalProtect App Configuration Setting	Description
Client Certificate Store Lookup	<p>Select the type of certificate or certificates that an agent or app looks up in its personal certificate store. The GlobalProtect agent or app uses the certificate to authenticate to the portal or a gateway and then establish a VPN tunnel to the GlobalProtect gateway.</p> <ul style="list-style-type: none"> • User—Authenticate by using the certificate that is local to the user's account. • Machine—Authenticate by using the certificate that is local to the endpoint. This certificate applies to all the user accounts permitted to use the endpoint. • User and machine (default)—Authenticate by using the user certificate and the machine certificate.
SCEP Certificate Renewal Period (days)	<p>This mechanism is for renewing a SCEP-generated certificate before the certificate actually expires. You specify the maximum number of days before certificate expiry that the portal can request a new certificate from the SCEP server in your PKI system (range is 0-30; default is 7). A value of 0 means that the portal does not automatically renew the client certificate when it refreshes a client configuration.</p> <p>For an agent or app to get the new certificate, the user must log in during the renewal period (the portal does not request the new certificate for a user during this renewal period unless the user logs in).</p> <p>For example, suppose that a client certificate has a lifespan of 90 days and this certificate renewal period is 7 days. If a user logs in during the final 7 days of the certificate lifespan, the portal generates the certificate and downloads it along with a refreshed client configuration. See GlobalProtect App Config Refresh Interval (hours).</p>
Extended Key Usage OID for Client Certificate	<p>Enter the extended key usage of a client certificate by specifying its object identifier (OID). This setting ensures that the GlobalProtect agent selects only a certificate that is intended for client authentication and enables GlobalProtect to save the certificate for future use.</p>
Enable Advanced View	<p>Select No to restrict the user interface on the client side to the basic, minimum view (enabled by default).</p>
Allow User to Dismiss Welcome Page	<p>Select No to force the Welcome Page to appear each time a user initiates a connection. This restriction prevents a user from dismissing important information, such as terms and conditions that may be required by your organization to maintain compliance.</p>
Enable Rediscover Network Option	<p>Select No to prevent users from manually initiating a network rediscovery.</p>
Enable Resubmit Host Profile Option	<p>Select No to prevent users from manually triggering resubmission of the latest HIP.</p>

GlobalProtect App Configuration Setting	Description
Allow User to Change Portal Address	<p>Select No to disable the Portal field on the Home tab in the GlobalProtect agent or app. However, because the user will then be unable to specify a portal to which to connect, you must supply the default portal address in the Windows registry or Mac plist:</p> <ul style="list-style-type: none"> • Windows registry HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup with key Portal • Mac plist /Library/Preferences/com.paloaltonetworks.GlobalProtect.pan.setup.plist with key Portal <p>For more information about pre-deploying the portal address, see Customizable Agent Settings in the GlobalProtect Administrator's Guide.</p>
Allow User to Continue with Invalid Portal Server Certificate	Select No to prevent the agent from establishing a connection with the portal if the portal certificate is not valid.
Display GlobalProtect Icon	Select No to hide the GlobalProtect icon on the client system. If the icon is hidden, users cannot perform certain tasks, such as viewing troubleshooting information, changing passwords, rediscovering the network, or performing an on-demand connection. However, HIP notification messages, login prompts, and certificate dialogs do display when user interaction is necessary.
User Switch Tunnel Rename Timeout (sec) (Windows Only)	<p>Specify the number of seconds that a remote user has to be authenticated by a GlobalProtect gateway after logging into an endpoint by using Microsoft's Remote Desktop Protocol (RDP) (range is 0-600; default is 0). Requiring the remote user to authenticate within a limited amount of time maintains security.</p> <p>After authenticating the new user and switching the tunnel to the user, the gateway renames the tunnel.</p> <p>A value of 0 means that the current user's tunnel is not renamed but, instead, is immediately terminated. In this case, the remote user gets a new tunnel and has no time limit for authenticating to a gateway (other than the configured TCP timeout).</p>
Show System Tray Notifications (Windows Only)	Select No to hide notifications from the user. Select Yes (default) to display notifications in the system tray area.
Custom Password Expiration Message (Windows Only)	Create a custom message to display to users when their password is about to expire. The maximum message length is 200 characters.
Maximum Internal Gateway Connection Attempts	Enter the maximum number of times the GlobalProtect agent should retry the connection to an internal gateway after the first attempt fails (range is 0-100; default is 0, which means the GlobalProtect agent does not retry the connection). By increasing the value, you enable the agent to automatically connect to an internal gateway that is temporarily down or unreachable during the first connection attempt but comes back up before the specified number of retries are exhausted. Increasing the value also ensures that the internal gateway receives the most up-to-date user and host information.
Portal Connection Timeout (sec)	The number of seconds before a connection request to the portal times out due to no response from the portal (range is 1-600; default is 30).

GlobalProtect App Configuration Setting	Description
TCP Connection Timeout (sec)	The number of seconds before a TCP connection request times out due to unresponsiveness from either end of the connection (range is 1-600; default is 60).
TCP Receive Timeout (sec)	The number of seconds before a TCP connection times out due to the absence of some partial response of a TCP request (range is 1-600; default is 30).
Update DNS Settings at Connect (Windows Only)	Select Yes to flush the DNS cache and force all adapters to use the DNS settings in the configuration. Select No (the default) to use the DNS settings of the client.
Detect Proxy for Each Connection (Windows Only)	Select No to auto-detect the proxy for the portal connection and use that proxy for subsequent connections. Select Yes (default) to auto-detect the proxy at every connection.
Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows Only)	Select No to prevent the GlobalProtect agent from sending HIP data when the status of the Windows Security Center (WSC) changes. Select Yes (default) to immediately send HIP data when the status of the WSC changes.
Retain Connection on Smart Card Removal (Windows Only)	Select Yes to retain the connection when a user removes a smart card containing a client certificate. Select No (default), to terminate the connection when a user removes a smart card.

Disable GlobalProtect Agent or App

Passcode/Confirm Passcode	Enter and then confirm a passcode if the setting for Allow User to Disable GlobalProtect App is Allow with Passcode . Treat this passcode like a password—record it and store it in a secure place. You can distribute the passcode to new GlobalProtect users by email or post it in a support area of your company website. If circumstances prevent the endpoint from establishing a VPN connection and this feature is enabled, a user can enter this passcode in the agent or app interface to disable the GlobalProtect agent and get Internet access without using the VPN.
Max Times User Can Disable	Specify the maximum number of times that a user can disable GlobalProtect before the user must connect to a firewall. The default value of 0 means users have no limit to the number of times they can disable the agent.
Disable Timeout (min)	Specify the maximum number of minutes the GlobalProtect agent or app can be disabled. After the specified time passes, the agent tries to connect to the firewall. The default of 0 indicates that the disable period is unlimited.

GlobalProtect App Configuration Setting	Description
Mobile Security Manager Settings	
Mobile Security Manager	If you are using the GlobalProtect Mobile Security Manager for mobile device management (MDM), enter the IP address or FQDN of the device check-in (enrollment) interface on the GP-100 appliance.
Enrollment Port	The port number the mobile endpoint should use when connecting to the GlobalProtect Mobile Security Manager for enrollment. By default, the Mobile Security Manager listens on port 443. A best practice is to keep this port number so that mobile endpoint users are not prompted for a client certificate during the enrollment process (possible values are 443, 7443, and 8443; default is 443).

GlobalProtect Portals Agent Data Collection Tab

Select **Network > GlobalProtect > Portals > <GlobalProtect-portal-config> > Agent > <agent-config> > Data Collection** to define the data the agent collects from the client in the HIP report.

GlobalProtect Data Collection Configuration Setting	Description
Collect HIP Data	Clear this selection to prevent the agent from collecting and sending HIP data.
Max Wait Time (sec)	Specify how many seconds the agent or app should search for HIP data before submitting the available data (range is 10-60; default is 20).
Exclude Categories	Select Exclude Categories to specify the host information categories for which you do not want the agent or app to collect HIP data. Select a Category (such as data-loss-prevention) to exclude from HIP collection. After selecting a category, you can Add and a particular Vendor and, then, you can Add specific products from the vendor to further refine the exclusion as needed. Click OK to save settings in each dialog.
Custom Checks	Select Custom Checks to define custom host information you want the agent to collect. For example, if you have any required applications that are not included in the Vendor or Product lists for creating HIP objects, you can create a custom check to determine whether that application is installed (it has a corresponding Windows registry or Mac plist key) or is currently running (has a corresponding running process): <ul style="list-style-type: none"> • Windows—Add a check for a particular registry key or key value. • Mac—Add a check for particular plist key or key value. • Process List—Add the processes you want to check for on user endpoints to see if they are running. For example, to determine whether a software application is running, add the name of the executable file to the process list. You can add a process to the Windows tab, the Mac tab, or both.

GlobalProtect Portals Satellite Configuration Tab

A satellite is a Palo Alto Networks firewall—typically at a branch office—that acts as a GlobalProtect agent to enable the satellite to establish VPN connectivity to a GlobalProtect gateway. Like a GlobalProtect agent, a satellite receives its initial configuration from the portal, which includes the certificates and VPN configuration routing information and enable the satellite to connect to all configured gateways to establish VPN connectivity.

Before configuring the GlobalProtect satellite settings on the branch office firewall, you must configure an interface with WAN connectivity and set up a security zone and policy to allow the branch office LAN to communicate with the Internet. You can then select **Network > GlobalProtect > Portals > <GlobalProtect-portal-config> > Satellite > <GlobalProtect-satellite>** to configure the GlobalProtect satellite settings on the portal, as in the following table.

GlobalProtect Portal Satellite Configuration Setting	Description
General	<ul style="list-style-type: none"> • Name—A name for this satellite configuration on the GlobalProtect portal. • Configuration Refresh Interval (hours)—How often a satellite should check the portal for configuration updates (range is 1-48; default is 24).
Devices	<p>Add a satellite using the firewall serial number. The portal can accept a serial number or login credentials to identify who is requesting a connection; if the portal does not receive a serial number, it requests login credentials. If you identify the satellite by its firewall serial number, you do not need to provide user login credentials when the satellite first connects to acquire the authentication certificate and its initial configuration.</p> <p>After the satellite authenticates by either a serial number or login credentials, the satellite hostname is automatically added to the portal.</p>
Enrollment User/User Group	<p>The portal can use Enrollment User/User Group settings with or without serial numbers to match a satellite to this configuration. Satellites that do not match on a serial number are required to authenticate either as an individual user or group member.</p> <p>Add the user or group that you want to receive this configuration.</p>  Before you can restrict the configuration to specific groups, you must enable Group Mapping in the firewall (Device > User Identification > Group Mapping Settings).

GlobalProtect Portal Satellite Configuration Setting	Description
Gateways	<p>Click Add to enter the IP address or hostname of the gateway(s) satellites by which this configuration can establish IPSec tunnels. Enter the FQDN or IP address of the interface where the gateway is configured in the Gateways field.</p> <p>(Optional) If you are adding two or more gateways to the configuration, the Routing Priority helps the satellite pick the preferred gateway (range is 1-25). Lower numbers have higher priority (for gateways that are available). The satellite multiplies the routing priority by 10 to determine the routing metric.</p>  Routes published by the gateway are installed on the satellite as static routes. The metric for the static route is 10 times the routing priority. If you have more than one gateway, be sure to set the routing priority so that routes advertised by backup gateways have higher metrics than the same routes advertised by primary gateways. For example, if you set the routing priority for the primary gateway and backup gateway to 1 and 10 respectively, the satellite will use 10 as the metric for the primary gateway and 100 as the metric for the backup gateway.
Trusted Root CA	<p>Click Add and then select the CA certificate for issuing gateway server certificates. As a best practice, all your gateways should use the same issuer.</p>  You can Import or Generate a root CA certificate for issuing gateway server certificates if one doesn't already exist on the portal.
Client Certificate	
Local	<ul style="list-style-type: none"> Issuing Certificate—Select the root CA issuing certificate the portal will use to issue certificates to a satellite after it successfully authenticates. If the needed certificate does not already exist on the firewall, you can Import or Generate it.  If the a certificate does not already reside on the firewall, you can Import or Generate an issuing certificate. <ul style="list-style-type: none"> Validity Period (days)—Specify the GlobalProtect satellite certificate lifetime (range is 7-365; default is 7). Certificate Renewal Period (days)—Specify the number of days before expiration that certificates can be automatically renewed (range is 3-30; default is 3). OCSP Responder—Select the OCSP Responder the satellite will use to verify the revocation status of certificates presented by the portal and gateways. None means that OCSP is not used for verifying revocation of a certificate.
SCEP	<ul style="list-style-type: none"> SCEP—Select a SCEP profile for generating client certificates. If the profile is not in the drop-down, you can create a New profile. Certificate Renewal Period (days)—Specify the number of days before expiration that certificates can be automatically renewed (range is 3-30; default is 3).

Network > GlobalProtect > Gateways

Select **Network > GlobalProtect > Gateways** to configure a GlobalProtect gateway. A gateway can provide VPN connections for GlobalProtect agents or apps or for GlobalProtect satellites.

From the GlobalProtect Gateway dialog, **Add** a new gateway configuration or select an existing gateway configuration to modify it.

What do you want to know?	See:
What general settings can I configure for the GlobalProtect gateway?	GlobalProtect Gateways General Tab
How do I configure the gateway client authentication?	GlobalProtect Gateways Authentication Tab
How do I configure the tunnel and network settings that enable an agent or app to establish a VPN tunnel with the gateway?	GlobalProtect Gateways Agent Tab
How do I configure the tunnel and network settings to enable the satellites to establish VPN connections with a gateway acting as a satellite?	GlobalProtect Gateways Satellite Configuration Tab
Looking for more?	For detailed, step-by-step instructions on setting up the portal, refer to Configure GlobalProtect Gateways in the <i>GlobalProtect Administrator's Guide</i> .

GlobalProtect Gateways General Tab

Select **Network > GlobalProtect > Gateways > General** to define the gateway interface to which the agents or apps can connect and specify how the gateway authenticates endpoint clients.

GlobalProtect Gateway General Setting	Description
Name	Enter a name for the gateway (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in multiple virtual system mode, the Location is the virtual system (vsys) where the GlobalProtect gateway is available. For a firewall that is not in multi-vsys mode, the Location field does not appear in the GlobalProtect Gateway dialog.  After you save the gateway configuration, you cannot change the Location .
Network Settings Area	
Interface	Select the name of the firewall interface that will serve as the ingress interface for remote endpoints. (These interfaces must already exist.)
IP Address	(Optional) Specify the IP address for gateway access.

GlobalProtect Gateways Authentication Tab

Select **Network > GlobalProtect > Gateways > Authentication** to identify the SSL/TLS service profile and to configure the details of client authentication. You can add multiple client authentication configurations.

GlobalProtect Gateway Authentication Setting	Description
SSL/TLS Service Profile	Select an SSL/TLS service profile for securing this GlobalProtect gateway. For details about the contents of a service profile, see Device > Certificate Management > SSL/TLS Service Profile .
Client Authentication Area	
Name	Enter a unique name to identify this configuration.
OS	By default, the configuration applies to all clients. You can refine the list of client endpoints by OS (Android , Chrome , iOS , Mac , Windows , or WindowsUWP), by Satellite devices, or by third-party IPSec VPN clients (X-Auth). The OS is the main differentiator between multiple configurations. If you need multiple configurations for one OS, you can further distinguish the configurations by your choice of authentication profile. A best practice is to order the configurations from most specific at the top of the list to most general at the bottom.
Authentication Profile	Choose an authentication profile or sequence from the drop-down to authenticate access to the gateway. Refer to Device > Authentication Profile .
Authentication Message	To help end users know what credentials they should use for logging into this gateway, you can enter a message or keep the default message. The message can have a maximum of 100 characters.

GlobalProtect Gateways Agent Tab

Select **Network > GlobalProtect > Gateways > Agent** to configure the tunnel settings that enable an agent or app to establish a VPN tunnel with the gateway. In addition, this tab lets you specify timeouts for VPNs, network services of DNS and WINS, and HIP notification messages for end users upon matching or not matching a HIP profile attached to a security policy.

Configure Agent settings on the following tabs:

- [GlobalProtect Gateways Agent Tunnel Settings Tab](#)
- [GlobalProtect Gateways Agent Timeout Settings Tab](#)
- [GlobalProtect Gateways Agent Client Settings Tab](#)
- [GlobalProtect Gateways Agent Network Services Tab](#)
- [GlobalProtect Gateways Agent HIP Notification Tab](#)

GlobalProtect Gateways Agent Tunnel Settings Tab

Select **Network > GlobalProtect > Gateways > Agent > Tunnel Settings** to enable tunneling and configure the tunnel parameters.

Tunnel parameters are required if you are setting up an external gateway. If you are configuring an internal gateway, tunnel parameters are optional.

GlobalProtect Gateway Client Tunnel Mode Configuration Setting	Description
Tunnel Mode	<p>Select Tunnel Mode to enable tunnel mode and then specify the following settings:</p> <ul style="list-style-type: none"> • Tunnel Interface—Choose a tunnel interface for access to this gateway. • Max User—Specify the maximum number of users that can simultaneously access the gateway for authentication, HIP updates, and GlobalProtect agent and app updates. If the maximum number of users is reached, subsequent users are denied access with a message that indicates the maximum number of users has been reached (range varies based on the platform and is displayed when the field is empty; by default, there is no limit). • Enable IPSec—Select this option to enable IPSec mode for client traffic, making IPSec the primary method and SSL-VPN the fallback method. The remaining options are not available until IPSec is enabled. • GlobalProtect IPSec Crypto—Select a GlobalProtect IPSec Crypto profile that specifies authentication and encryption algorithms for the VPN tunnels. The default profile uses AES-128-CBC encryption and SHA1 authentication. For details, see Network > Network Profiles > GlobalProtect IPSec Crypto. If you Enable X-Auth Support, GlobalProtect IPSec Crypto profiles are not applicable. • Enable X-Auth Support—Select this option to enable Extended Authentication (X-Auth) support in the GlobalProtect gateway when IPSec is enabled. With X-Auth support, third party IPSec VPN clients that support X-Auth (such as the IPSec VPN client on Apple iOS and Android devices and the VPNC client on Linux) can establish a VPN tunnel with the GlobalProtect gateway. The X-Auth option provides remote access from the VPN client to a specific GlobalProtect gateway. Because X-Auth access provides limited GlobalProtect functionality, consider using the GlobalProtect App for simplified access to the full security feature set GlobalProtect provides on iOS and Android devices. <p>Selecting X-Auth Support activates the Group Name and Group Password options:</p> <ul style="list-style-type: none"> • If the group name and group password are specified, the first authentication phase requires both parties to use this credential to authenticate. The second phase requires a valid username and password, which is verified through the authentication profile configured in the Authentication section. • If no group name and group password are defined, the first authentication phase is based on a valid certificate presented by the third-party VPN client. This certificate is then validated through the certificate profile configured in the authentication section. • By default, the user is not required to re-authenticate when the key used to establish the IPSec tunnel expires. To require the user to re-authenticate, clear the Skip Auth on IKE Rekey option.

GlobalProtect Gateways Agent Timeout Settings Tab

Select **Network > GlobalProtect > Gateways > Agent > Timeout Settings** to define the maximum value that a user session or tunnel connection can be idle.

GlobalProtect Gateway Client Tunnel Mode Timeout Settings
Specify the following timeout settings:
<ul style="list-style-type: none"> • 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 specified amount of time.

GlobalProtect Gateways Agent Client Settings Tab

Select **Network > GlobalProtect > Gateways > Agent > Client Settings** to configure settings for the virtual network adapter on the client system when an agent establishes a tunnel with the gateway.



Some **Client Settings** options are available only after you enable tunnel mode and define a tunnel interface on the [GlobalProtect Gateways Agent Tunnel Settings Tab](#).

GlobalProtect Gateway Client Setting or Network Configuration	Description
Authentication	
Name	Enter a name to identify the client settings configuration (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Authentication Override	<p>Enable the gateway to use secure, device-specific, encrypted cookies to authenticate the user after the user first authenticates using the authentication scheme specified by the authentication or certificate profile.</p> <ul style="list-style-type: none"> • Generate cookie for authentication override—During the lifetime of the cookie, the agent presents this cookie each time the user authenticates with the gateway. • Cookie Lifetime—Specify the hours, days, or weeks that the cookie is valid. The typical lifetime is 24 hours. The ranges are 1–72 hours, 1–52 weeks, or 1–365 days. After the cookie expires, the user must enter login credentials and the gateway subsequently encrypts a new cookie to send to user device. • Accept cookie for authentication override—Select this option to configure the gateway to accept authentication using the encrypted cookie. When the agent presents the cookie, the gateway validates that the cookie was encrypted by the gateway before authenticating the user. • Certificate to Encrypt/Decrypt Cookie—Select the certificate the gateway uses to use when encrypting and decrypting the cookie. <p> Ensure that the gateway and portal both use the same certificate to encrypt and decrypt cookies.</p>

GlobalProtect Gateway Client Setting or Network Configuration	Description
User/User Group tab	Specify the user or user group and client operating system to which this agent configuration applies.
User/User Group	<p>Add a specific user or user group to which this configuration applies.</p>  <p>You must configure group mapping (Device > User Identification > Group Mapping Settings) before you can select users and groups.</p> <p>You can also create configurations that are deployed to agents or apps in pre-logon mode (before the user logs in to the endpoint) or configurations to deploy to any user.</p>
OS	To deploy configurations based on the operating system running on the endpoint, Add an OS (Android, Chrome, iOS, Mac, Windows, or WindowsUWP) . Alternatively, you can leave this value set to Any so that configuration deployment is based only on the user or user group and not on the operating system of the endpoint.
Network Settings tab	
Retrieve Framed-IP-Address attribute from authentication server	Select this option to enable the GlobalProtect gateway to assign fixed IP addresses by use of an external authentication server. When this option is enabled, the GlobalProtect gateway allocates the IP address for connecting to devices by using the Framed-IP-Address attribute from the authentication server.
Authentication Server IP Pool	<p>Add a subnet or range of IP addresses to assign to remote users. When the tunnel is established, the GlobalProtect gateway allocates the IP address in this range to connecting devices using the Framed-IP-Address attribute from the authentication server.</p> <p>You can enable and configure Authentication Server IP Pool only if you enable Retrieve Framed-IP-Address attribute from authentication server.</p>  <p>The authentication server IP pool must be large enough to support all concurrent connections. IP address assignment is fixed and is retained after the user disconnects. Configure multiple ranges from different subnets to allow the system to offer clients an IP address that does not conflict with other interfaces on the client.</p> <p>The servers and routers in the networks must route the traffic for this IP pool to the firewall. For example, for the 192.168.0.0/16 network, a remote user can receive the address 192.168.0.10.</p>
IP Pool	<p>Add a range of IP addresses to assign to remote users. When the tunnel is established, an interface is created on the remote user's computer with an address in this range.</p>  <p>To avoid conflicts, the IP pool must be large enough to support all concurrent connections. The gateway maintains an index of clients and IP addresses so that the client automatically receives the same IP address the next time it connects. Configuring multiple ranges from different subnets allows the system to offer clients an IP address that does not conflict with other interfaces on the client.</p> <p>The servers and routers in the networks must route the traffic for this IP pool to the firewall. For example, for the 192.168.0.0/16 network, a remote user may be assigned the address 192.168.0.10.</p>

GlobalProtect Gateway Client Setting or Network Configuration	Description
No direct access to local network	Select this option to disable split tunneling, including direct access to local networks on Windows and Mac OS endpoints. This function prevents a user from sending traffic to proxies or local resources, such as a home printer. When the tunnel is established, all traffic is routed through the tunnel and is subject to policy enforcement by the firewall.
Access Route	Add routes that the gateway pushes to the remote users' endpoint and thereby determine what the users' endpoint can 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 you don't add a route, 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 of the user's endpoint and gaining access to the internal network (with the user's endpoint acting as a bridge).

GlobalProtect Gateways Agent Network Services Tab

Select **Network > GlobalProtect > Gateways > Agent > Network Services** to 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.



Network Services options are available only if you have enable tunnel mode and define a tunnel interface on the [GlobalProtect Gateways Agent Tunnel Settings Tab](#).

GlobalProtect Gateway Client Network Services Configuration Setting	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' or apps' configuration. With this setting, all client network configurations, such as DNS servers and WINS servers, are inherited from the configuration of the interface selected in the Inheritance Source.
Check inheritance source status	Click Inheritance Source to see the server settings that are currently assigned to the client interfaces.
Primary DNS Secondary DNS	Enter the IP addresses of the primary and secondary servers that provide DNS to the clients.
Primary WINS Secondary WINS	Enter the IP addresses of the primary and secondary servers that provide Windows Internet Naming Service (WINS) to the clients.
DNS Suffix	Add 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 option to inherit the DNS suffixes from the inheritance source.

GlobalProtect Gateways Agent HIP Notification Tab

Select **Network > GlobalProtect > Gateways > Agent > HIP Notification** to define the notification messages that end users see when a security rule with a host information profile (HIP) is enforced.

These options are available only if you created HIP Profiles and added them to your security policies.

GlobalProtect Client HIP Notification Configuration Setting	Description
HIP Notification	<p>Add HIP Notifications and configure the options. You can Enable notifications for the Match Message, the Not Match Message, or both and then specify whether to Show Notification As a System Tray Balloon or a Pop Up Message. Then specify the message to match or not match.</p> <p>Use these settings to notify the end user about the state of the machine, such as a warning message that the host system does not have a required application installed. For the Match Message, you can also enable the option to Include Mobile App List to indicate what applications triggered the HIP match.</p>  You can format HIP notification messages in rich HTML, which allows you to include links to external web sites and resources. Click hyperlink () in the rich text settings toolbar to add links.

GlobalProtect Gateways Satellite Configuration Tab

A satellite 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. Select **Network > GlobalProtect > Gateways > Satellite Configuration** to define the gateway tunnel and network settings to enable the satellites to establish VPN connections with it. You can also configure routes advertised by the satellites.

- [GlobalProtect Gateways Satellite Tunnel Settings tab](#)
- [GlobalProtect Gateways Satellite Network Settings tab](#)
- [GlobalProtect Gateways Satellite Route Filter tab](#)

The following table describes the GlobalProtect gateway satellite configuration settings.

GlobalProtect Gateway Satellite Configuration Setting	Description
GlobalProtect Gateways Satellite Tunnel Settings tab	
Tunnel Configuration	<p>Select Tunnel Configuration and select an existing Tunnel Interface, or select New Tunnel Interface from the drop-down. See Network > Interfaces > Tunnel for more information.</p> <ul style="list-style-type: none"> • 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 to preserve the original ToS information. • Configuration refresh interval (hours)—Specify how often satellites should check the portal for configuration updates (range is 1-48; default is 2).

GlobalProtect Gateway Satellite Configuration Setting	Description
Tunnel Monitoring	<p>Select Tunnel Monitoring to enable the satellites to monitor gateway tunnel connections, allowing them to failover to a backup gateway if the connection fails.</p> <ul style="list-style-type: none"> • 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 LVPN.
Crypto Profiles	Select an IPSec Crypto Profile or create a new one. A crypto profile determines the protocols and algorithms for identification, authentication, and encryption for the VPN tunnels. Because both tunnel endpoints in an LVPN are trusted firewalls within your organization, you typically use the default profile, which uses ESP protocol, DH group2, AES 128 CVC encryption, and SHA-1 authentication. See Network > Network Profiles > GlobalProtect IPSec Crypto for more details.

GlobalProtect Gateways Satellite Network Settings tab

Inheritance Source	Select a source to propagate DNS server and other settings from the selected DHCP client or PPPoE client interface into the GlobalProtect satellite configuration. With this setting, all network configuration, such as DNS servers, are inherited from the configuration of the interface selected in the Inheritance Source.
Primary DNS Secondary DNS	Enter the IP addresses of the primary and secondary servers that provide DNS to the satellites.
DNS Suffix	Click Add to enter a suffix that the satellite should use locally when an unqualified hostname is entered that it cannot resolve. You can enter multiple suffixes by separating them with commas.
Inherit DNS Suffix	Select this option to send the DNS suffix to the satellites to use locally when an unqualified hostname is entered that it cannot resolve.
IP Pool	<p>Add a range of IP addresses to assign to the tunnel interface on satellites upon establishment of the VPN tunnel.</p>  <p>The IP pool must be large enough to support all concurrent connections. IP address assignment is dynamic and not retained after the satellite disconnects. Configuring multiple ranges from different subnets will allow the system to offer satellites an IP address that does not conflict with other interfaces on the satellites.</p> <p>The servers and routers in the networks must route the traffic for this IP pool to the firewall. For example, for the 192.168.0.0/16 network, a satellite can be assigned the address 192.168.0.10.</p> <p>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.</p>

GlobalProtect Gateway Satellite Configuration Setting	Description
Access Route	<p>Click Add and then enter routes as follows:</p> <ul style="list-style-type: none"> • 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 <i>split tunneling</i>), specify the destination subnets that must be tunneled. In this case, the satellite routes traffic that is not destined for a specified access route by using its own routing table. For example, you can choose to tunnel only the traffic destined for your corporate network and use the local satellite to enable safe Internet access. • If you want to enable routing between satellites, enter the summary route for the network protected by each satellite.

GlobalProtect Gateways Satellite Route Filter tab

Enable **Accept published routes** to accept routes advertised by the satellite into the gateway's routing table. If you do not select this option, the gateway does not accept any routes advertised by the satellites.

If you want to be more restrictive about accepting the routes advertised by the satellites, **Add Permitted subnets** and define the subnets from which the gateway may accept routes; subnets advertised by the satellites that are not part of the list are filtered out. For example, if all the satellites are configured with 192.168.x.0/24 subnet on the LAN side, you can configure a permitted route of 192.168.0.0/16 on the gateway. This configuration causes the gateway to accept the routes from the satellite only if it is in the 192.168.0.0/16 subnet.

Network > GlobalProtect > MDM

If you are using a Mobile Security Manager to manage end user mobile 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.

For more detailed information on setting up the GlobalProtect Mobile Security Manager service, refer to [Set Up the GlobalProtect Mobile Security Manager](#) in the *GlobalProtect 6.2 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](#).

Add MDM information for the Mobile Security Manager to enable the gateway to communicate with the Mobile Security Manager.

GlobalProtect MDM Setting	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 multi-vsys 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 connects to retrieve HIP reports. Ensure that you have a service route to this interface.
Connection Port	The connection port is where the Mobile Security Manager listens for HIP report requests. The default port is 5008, which is the same port on which the GlobalProtect Mobile Security Manager listens. If you are using a third-party Mobile Security Manager, enter the port number on which that server listens for HIP report requests.
Client Certificate	Choose the client certificate for the gateway to present to the Mobile Security Manager when it establishes an HTTPS connection. This certificate is required only if the Mobile Security Manager is configured to use mutual authentication.
Trusted Root CA	Click Add and then select the root CA certificate that was used to issue the certificate for the interface where the gateway connects to retrieve HIP reports. (This server certificate can be different from the certificate issued for the device check-in interface on the Mobile Security Manager). You must import the root CA certificate and add it to this list.

Network > GlobalProtect > Block List

Select **Network > GlobalProtect > Device Block List (firewall only)** to add devices to the GlobalProtect device block list. Devices on this list are not permitted to establish a GlobalProtect VPN connection.

Device Block List Setting	Description
Name	Enter a name for the device block list (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in multiple virtual system mode, the Location is the virtual system (vsys) where the GlobalProtect gateway is available. For a firewall that is not in multi-vsys mode, the Location field does not appear in the GlobalProtect Gateway dialog. After you save the gateway configuration, you cannot change the Location .
Host ID	Enter the unique ID that identifies the client, a combination of host name and unique device ID. For each Host ID, specify the corresponding Hostname.
Hostname	Enter a hostname to identify the device (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

Objects > GlobalProtect > HIP Objects

Select **Objects > GlobalProtect > HIP Objects** to define objects for a host information profile (HIP). HIP objects provide the matching criteria for filtering the raw data reported by an agent or app that you want to use to enforce policy. For example, if the raw host data includes information about several antivirus packages on a client, you might be interested in a particular application because your organization requires that package. For this scenario, you create a HIP object to match the specific application you want to enforce.

The best way to determine the HIP objects you need is to determine how you will use the host information to enforce policy. Keep in mind that the HIP objects are merely building blocks that allow you to create the HIP profiles that your security policies can use. Therefore, you may want to keep your objects simple, matching on one thing, such as the presence of a particular type of required software, membership in a specific domain, or the presence of a specific client OS. With this approach, you have the flexibility to create a very granular, HIP-augmented policy.

To create a HIP object, click **Add** to open the HIP Object dialog. For a description of what to enter in a specific field, see the tables that follow.

- [HIP Objects General Tab](#)
- [HIP Objects Mobile Device Tab](#)
- [HIP Objects Patch Management Tab](#)
- [HIP Objects Firewall Tab](#)
- [HIP Objects Antivirus Tab](#)
- [HIP Objects Anti-Spyware Tab](#)
- [HIP Objects Disk Backup Tab](#)
- [HIP Objects Disk Encryption Tab](#)
- [HIP Objects Data Loss Prevention Tab](#)
- [HIP Objects Custom Checks Tab](#)

For more detailed information on creating HIP-augmented security policies, refer to [Configure HIP-Based Policy Enforcement](#) in the *GlobalProtect Administrator's Guide*.

HIP Objects General Tab

Select **Objects > GlobalProtect > HIP Objects > General** to specify a name for the new HIP object and configure the object to match against general host information such as domain, operating system, or type of network connectivity.

HIP Object General Setting	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	<p>If you select Shared, the current HIP objects become available to:</p> <ul style="list-style-type: none"> Every virtual system (vsys) on the firewall, if you are logged in to a firewall that is in multiple virtual system mode. If you clear this selection, the object will be available to only the vsys selected in the Virtual System drop-down of the Objects tab. For a firewall that is not in multi-vsys mode, this option is not available in the HIP Object dialog. All device groups on Panorama™. If you clear this selection, the object will be available only to the device group selected in the Device Group drop-down of the Objects tab. <p>After you save the object, you cannot change its Shared setting. Select Objects > GlobalProtect > HIP Objects to see the current Location.</p>
Description	Enter an optional description.
Disable override (Panorama only)	Controls override access to the HIP object in the device groups that are descendants of the Device Group selected in the Objects tab. Select this option to prevent administrators from creating local copies of the object in descendant device groups by overriding its inherited values. This option is cleared by default (override is enabled).
Host Info	Select this option to activate the options for configuring the host information.
Domain	To match on a domain name, choose an operator from the drop-down and enter a string to match.
OS	To match on a host OS, choose Contains from the first drop-down, select a vendor from the second drop-down, and then select an OS version from the third drop-down; or you can select All to match on any OS version from the selected vendor.
Client 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.

HIP Object General Setting	Description
Host Name	To match on a specific host name or part of a host name, select an operator from the drop-down and then enter a string to match (or not match, depending on what operator you selected) in the text box.
Host ID	The host ID is a unique ID that GlobalProtect assigns to identify the host. The host ID value varies by device type: <ul style="list-style-type: none"> Windows—Machine GUID stored in the Windows registry (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid) macOS—MAC address of the first built-in physical network interface Android—Android ID iOS—UDID Chrome—GlobalProtect assigned unique alphanumeric string with length of 32 characters To match on a specific host ID, select the operator from the drop-down and then enter a string to match (or not match, depending on what operator you selected) in the text box.
Network	Use this field to enable filtering on a specific mobile device network configuration. This match criteria applies to mobile devices only. Select an operator from the drop-down and then select the type of network connection to filter on from the second drop-down— Wifi , Mobile , Ethernet (available only for Is Not filters), or Unknown . After you select a network type, enter any additional strings to match on, if available, such as the Mobile Carrier or Wifi SSID .

HIP Objects Mobile Device Tab

Select **Objects > GlobalProtect > HIP Objects > Mobile Device** to enable HIP matching on data collected from mobile devices that run the GlobalProtect app.

HIP Object Mobile Device Setting	Description
Mobile Device	Select this option to enable filtering on host data collected from mobile devices that are running the GlobalProtect app and to enable the Device , Settings , and Apps tabs.
Device tab	<ul style="list-style-type: none"> 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.

HIP Object Mobile Device Setting	Description
Settings tab	<ul style="list-style-type: none"> 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 or jailbroken, select Yes. To match devices that have not been rooted or jailbroken, select No. Disk Encryption—Filter based on whether the device data has been encrypted. To match devices that have disk encryption enabled, select yes. To match devices that do not have disk encryption enabled, select no. Time Since Last Check-in—Filter based on when the device last checked in with the MDM. Select an operator from the drop-down and then specify the number of days for the check-in window. For example, you could define the object to match devices that have not checked in within the last 5 days.
Apps tab	<ul style="list-style-type: none"> Apps—(Android devices only) Select this option to enable filtering based on the apps that are installed on the device and whether or not the device has any malware-infected apps installed. Criteria tab Has Malware—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 tab 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.

HIP Objects Patch Management Tab

Select **Objects > GlobalProtect > HIP Objects > Patch Management** to enable HIP matching on the patch status of the GlobalProtect clients.

HIP Object Patch Management Setting	Description
Patch Management	Select this option to enable matching on the patch management status of the host and enable the Criteria and Vendor tabs.

HIP Object Patch Management Setting	Description
Criteria tab	<p>Specify the following settings:</p> <ul style="list-style-type: none"> • Is Installed—Match on whether patch management software is installed on the host. • Is Enabled—Match on whether patch management software is enabled on the host. If the Is Installed selection is cleared, this field is automatically set to None and is disabled for editing. • Severity—Select from the list of logical operators for matching on whether the host has missing patches of the specified severity number. • Check—Match on whether the endpoint 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 tab	<p>Define specific vendors of patch management software and products to look for on the endpoint to determine a match. Click Add and then choose a Vendor from the drop-down. Optionally, click Add to choose a specific Product. Click OK to save the settings.</p>

HIP Objects Firewall Tab

Select **Objects > GlobalProtect > HIP Objects > Firewall** to enable HIP matching based on the firewall software status of the GlobalProtect clients.

HIP Object Firewall Settings
<p>Select Firewall to enable matching on the firewall software status of the host:</p> <ul style="list-style-type: none"> • Is Installed—Match on whether firewall software is installed on the host. • Is Enabled—Match on whether firewall software is enabled on the host. If the Is Installed selection is cleared, this field is automatically set to None and is disabled for editing. • Vendor and Product—Define specific firewall software vendors and/or products to look for on the host to determine a match. Click Add and then choose a Vendor from the drop-down. Optionally, click Add to choose a specific Product. Click OK to save the settings. • Exclude Vendor—Select this option to match hosts that do not have software from the specified vendor.

HIP Objects Antivirus Tab

Select **Objects > GlobalProtect > HIP Objects > Antivirus** to enable HIP matching based on the antivirus coverage on the GlobalProtect clients.

HIP Object Antivirus Settings

Select **Antivirus** to enable matching on the antivirus coverage on the host and then define additional matching criteria for the match as follows:

- **Is Installed**—Match on whether antivirus software is installed on the host.
- **Real Time Protection**—Match on whether real-time antivirus protection is enabled on the host. If the **Is Installed** selection is cleared, this field is automatically set to **None** and is disabled for editing.
- **Virus Definition Version**—Match when the virus definitions have been updated within a specified number of days or release versions.
- **Product Version**—Match a specific version of the antivirus software. To specify a version, select an operator from the drop-down and then enter a string representing the product version.
- **Last Scan Time**—Match 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** and then choose a **Vendor** from the drop-down. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings.
- **Exclude Vendor**—Select this option to match hosts that do not have software from the specified vendor.

HIP Objects Anti-Spyware Tab

Select **Objects > GlobalProtect > HIP Objects > Anti-Spyware** to enable HIP matching based on the anti-spyware coverage on the GlobalProtect clients.

HIP Object Anti-Spyware Settings

Select **Anti-Spyware** 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** selection 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**—Select an operator from the list and then enter the versions of virus definition to match. If the operator is **Within** or **Not Within**, specify a number of days or release versions.
- **Product Version**—Select an operator from the list and then enter the product version to match a specific version of anti-spyware software.
- **Last Scan Time**—Specify whether to match based on the time that the last anti-spyware scan ran. Select an operator and then specify a number of **Days** or **Hours** to match.
- **Vendor and Product**—Define specific anti-spyware software vendors or products to look for on the host to determine a match. Click **Add** and then choose a **Vendor** from the drop-down. Optionally, click **Add** to choose a specific **Product**. Click **OK** to save the settings.
- **Exclude Vendor**—Select this option to match hosts that do not have software from the specified vendor.

HIP Objects Disk Backup Tab

Select **Objects > GlobalProtect > HIP Objects > Disk Backup** to enable HIP matching based on the disk backup status of the GlobalProtect clients.

HIP Object Disk Backup Settings	
Select Disk Backup to enable matching on the disk backup status on the host and then define additional matching criteria for the match as follows:	
• Is Installed —Match on whether disk backup software is installed on the host.	
• Last Backup Time —Specify whether to match based on the time that the last disk backup was run. Select an operator from the drop-down and then specify a number of Days or Hours to match against.	
• Vendor and Product —Define specific disk backup software vendors and products to match on the host. Click Add and then choose a Vendor from the drop-down. Optionally, click Add to choose a specific Product . Click OK to save the settings.	
• Exclude Vendor —Select this option to match hosts that do not have software from the specified vendor.	

HIP Objects Disk Encryption Tab

Select **Objects > GlobalProtect > HIP Objects > Disk Encryption** to enable HIP matching based on the disk encryption status of the GlobalProtect clients.

HIP Object Disk Encryption Setting	Description
Disk Encryption	Select Disk Encryption to enable matching on the disk encryption status on the host.
Criteria	Specify the following settings: <ul style="list-style-type: none">• Is Installed—Match on whether disk encryption software is installed on the host.• Encrypted Locations—Click Add to specify the drive or path to check for disk encryption when determining a match:• Encrypted Locations—Enter specific locations to check for encryption on the host.• State—Specify how to match the state of the encrypted location by choosing an operator from the drop-down and then selecting a possible state (full, none, partial, not-available).• Click OK to save the settings.
Vendor	Define specific disk encryption software vendors and products to match on the endpoint. Click Add and then choose a Vendor from the drop-down. Optionally, click Add to choose a specific Product . Click OK to save the settings and return to the Disk Encryption tab.

HIP Objects Data Loss Prevention Tab

Select **Objects > GlobalProtect > HIP Objects > Data Loss Prevention** to configure HIP matching that is based on whether the GlobalProtect clients are running data loss prevention software.

HIP Object Data Loss Prevention Settings	
Select Data Loss Prevention to enable matching on the data loss prevention (DLP) status on the host (Windows hosts only) and then define additional matching criteria for the match as follows:	
<ul style="list-style-type: none"> • Is Enabled—Match on whether DLP software is enabled on the host. If the Is Installed selection is cleared, this field is automatically set to None and is disabled for editing. • 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 and then choose a Vendor from the drop-down. Optionally, click Add to choose a specific Product. Click OK to save the settings. • Exclude Vendor—Select this option to match hosts that do not have software from the specified vendor. 	

HIP Objects Custom Checks Tab

Select **Objects > GlobalProtect > HIP Objects > Custom Checks** to enable HIP matching on any custom checks you have defined on the GlobalProtect portal. For details on adding the custom checks to the HIP collection, see [Network > GlobalProtect > Portals](#).

HIP Object Custom Checks Setting	Description
Custom Checks	Select Custom Checks to enable matching on custom checks you defined on the GlobalProtect portal.
Process List	To check the host system for a specific process, click Add and then enter the process name. By default, the agent checks for running processes; if you just want to see if a specific process is present on the system even if not running, clear the Running selection.
Registry Key	To check Windows hosts for a specific registry key, click Add and enter the Registry Key to match. To match only the hosts that lack the specified registry key or the key's value, mark the Key does not exist or match the specified value data box. To match on specific values, click Add and then enter the Registry Value and Value Data . To match hosts that explicitly do not have the specified value or value data, select Negate . Click OK to save the settings.
Plist	To check Mac hosts for a specific entry in the property list (plist), click Add and enter the Plist name. To match only the hosts that do not have the specified plist, select Plist does not exist . To match on specific key-value pair within the plist, click Add and then enter the Key and the corresponding Value to match. To match hosts that explicitly do not have the specified key or value, select Negate . Click OK to save the settings.

Objects > GlobalProtect > HIP Profiles

Select **Objects > GlobalProtect > HIP Profiles** to create the HIP profiles—a collection of HIP objects to be evaluated together either for monitoring or for security policy enforcement—that you use to set up HIP-enabled security policies. When creating HIP profiles, you can combine the HIP objects you previously created (as well as other HIP profiles) by using Boolean logic, so that when a traffic flow is evaluated against the resulting HIP profile, it will either match or not match. Upon a match, the corresponding policy rule is enforced; if there is no match, the flow is evaluated against the next rule (as with any other policy matching criteria).

To create a HIP profile, click **Add**. The following table provides information on what to enter in the fields in the HIP Profile dialog. For more detailed information on setting up GlobalProtect and the workflow for creating HIP-augmented security policies, refer to [Configure HIP-Based Policy Enforcement](#) in the *GlobalProtect Administrator's Guide*.

HIP Profile Setting	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 Shared to make the current HIP profile available to: <ul style="list-style-type: none">Every virtual system (vsys) on the firewall, if you are logged in to a firewall that is in multiple virtual system mode. If you clear this selection, the profile is available only to the vsys selected in the Virtual System drop-down on the Objects tab. For a firewall that is not in multi-vsys mode, this option does not appear in the HIP Profile dialog.All device groups on Panorama. If you clear this selection, the profile is available only to the device group selected in the Device Group drop-down on the Objects tab. After you save the profile, you cannot change its Shared setting. Select Objects > GlobalProtect > HIP Profiles to view the current Location .
Disable override (Panorama only)	Controls override access to the HIP profile in device groups that are descendants of the Device Group selected in the Objects tab. Select this option if you want to prevent administrators from creating local copies of the profile in descendant device groups by overriding its inherited values. This option is cleared by default (override is enabled).

HIP Profile Setting	Description
Match	<p>Click Add Match Criteria to open the HIP Objects/Profiles Builder. Select the first HIP object or profile you want to use as match criteria and then add () it to the Match text box on the HIP Objects/ProfilesBuilder dialog. Keep in mind that if you want the HIP profile to evaluate the object as a match only when the criteria in the object is not true for a flow, select NOT before adding the object.</p> <p>Continue adding match criteria as appropriate for the profile you are building, and ensure you select the appropriate Boolean operator (AND or OR) between each addition (and using the NOT operator when appropriate).</p> <p>To create a complex Boolean expression, you must manually add the parenthesis in the proper places in the Match text box to ensure that the HIP profile is evaluated using the intended logic. For example, the following expression indicates that the HIP profile will match traffic from a host that has either FileVault disk encryption (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:</p> <pre>(("MacOS" and "FileVault") or ("Windows" and "TrueCrypt")) and "Domain" and "SymantecAV"</pre> <p>When you have finished adding the objects and profiles to the new HIP profile, click OK.</p>

Device > GlobalProtect Client

The following topics describe how to set up and manage the Global Protect agent.

What do you want to know?	See:
View more information about the GlobalProtect agent software releases.	Managing the GlobalProtect Agent Software
Install the GlobalProtect agent software.	Setting Up the GlobalProtect Agent
Use the GlobalProtect agent software.	Using the GlobalProtect Agent
Looking for more?	For detailed, step-by-step instructions on setting up the GlobalProtect client software, refer to Deploy the GlobalProtect Client Software in the <i>GlobalProtect Administrator's Guide</i> .

Managing the GlobalProtect Agent Software

Select **Device > GlobalProtect Client (firewall only)** to download and activate the GlobalProtect agent software on the firewall that hosts the portal. Thereafter, endpoints that connect to the portal download the agent software. In the agent configurations you specify on the portal, you define how and when the portal pushes software to endpoints. Your configuration determines whether upgrades occur automatically when the agent connects, whether end users are prompted to upgrade, or whether upgrading is prohibited for all or a particular set of users. See [Allow User to Upgrade GlobalProtect App](#) for more details. For details on the options for distributing the GlobalProtect 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 the initial download and installation of the GlobalProtect agent, the user of the client endpoint must be logged in with administrator rights. For subsequent upgrades, administrator rights are not required.

GlobalProtect Client Setting	Description
Version	This version number is of the GlobalProtect agent software that is available on the Palo Alto Networks Update Server. To see if a new agent software release is available from Palo Alto Networks, click Check Now . The firewall uses its service route to connect to the Update Server to determine if new versions are available and displays them at the top of the list.
Size	The size of the 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.

GlobalProtect Client Setting	Description
Action	<p>Indicates the current action you can take for the corresponding agent software package as follows:</p> <ul style="list-style-type: none"> • Download—The corresponding agent software version is available on the Palo Alto Networks Update Server. Click Download to initiate the download. If the firewall does not have access to the Internet, use an Internet-connected computer to go to the Software Update site to look for and Download new agent software versions to your local computer. Then 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 Activate to activate the software and enable agent upgrade. To activate a software update you manually uploaded to the firewall, click Activate From File and select the version you want to activate from the drop-down (you may need to refresh the screen for it to show as Currently Activated). • Reactivate—The corresponding agent software has been activated and is ready for the client to 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 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).



Be sure to choose the correct installation option for your host operating system (32-bit or 64-bit). If you are installing on a 64-bit host, use the 64-bit browser and Java combination for the initial installation.

To install the agent, open the installer file and follow the on-screen instructions.

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.

- **Home tab**—Allows users to change the portal IP address or hostname and enter their authentication credentials. Also 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 the user 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.



Panorama Web Interface

Panorama™ is the centralized management system for the Palo Alto Networks® family of next-generation firewalls. It provides a single location from which you can oversee all applications, users, and content traversing your network, and then use this knowledge to create policies that protect and control the network. Using Panorama for centralized policy and firewall management increases operational efficiency in administering and maintaining a distributed firewall network. Panorama is available both as a dedicated hardware platform (M-Series appliance) and as a VMware virtual appliance (running on an ESXi server or vCloud Air).

While many Panorama web interface pages and settings are identical to those on the firewall web interface, this section describes options that are exclusively available on the Panorama web interface to manage Panorama, firewalls, and log collectors.

- ▲ [Use the Panorama Web Interface](#)
- ▲ [Commit Your Changes in Panorama](#)
- ▲ [Defining Policies on Panorama](#)
- ▲ [Logs and Reports on Panorama](#)
- ▲ [Log Storage Partitions for a Panorama Virtual Appliance](#)
- ▲ [Panorama > High Availability](#)
- ▲ [Panorama > Administrators](#)
- ▲ [Panorama > Admin Roles](#)
- ▲ [Panorama > Access Domains](#)
- ▲ [Panorama > Managed Devices](#)
- ▲ [Panorama > Templates](#)
- ▲ [Panorama > Device Groups](#)
- ▲ [Panorama > Managed Collectors](#)
- ▲ [Panorama > Collector Groups](#)
- ▲ [Panorama > VMware Service Manager](#)
- ▲ [Panorama > Log Settings](#)
- ▲ [Panorama > Scheduled Config Export](#)
- ▲ [Panorama > Software](#)
- ▲ [Panorama > Device Deployment](#)

Looking for more?

See the [Panorama Administrator's Guide](#) for details on setting up and using Panorama for centralized management.

Use the Panorama Web Interface

The web interfaces of Panorama and the firewall have the same look and feel. However, the Panorama web interface has additional options for managing Panorama and for using Panorama to manage firewalls and Log Collectors.

You can use the **Context** drop-down above the side menu to switch between the Panorama web interface and a firewall web interface. When you select a firewall, the web interface refreshes to show all the pages and options for the selected firewall so that you can manage it locally. The drop-down displays only the firewalls to which you have administrative access (see [Panorama > Access Domains](#)) and that are connected to Panorama. The icons of firewalls that are in high availability (HA) mode will have colored backgrounds to indicate their HA state .

Panorama Page	Description
Setup	<p>Enables you to:</p> <ul style="list-style-type: none"> Specify general settings (for example, the Panorama host name). Specify settings for authentication, the management interface, logs, reports, AutoFocus, banners, the message of the day, and password complexity. Back up and restore configurations. Define network server connections (DNS and NTP). Select the WildFire server. Manage hardware security module (HSM) settings. <p>Select Device > Setup > Management.</p>
High Availability	Enables you to configure high availability (HA) for a pair of Panorama management servers. Select Panorama > High Availability .
Config Audit	Enables you to see the differences between configuration files. Select Device > Config Audit .
Password Profiles	Enables you to define password profiles for Panorama administrators. Select Device > Password Profiles .
Administrators	<p>Enables you to configure Panorama administrator accounts. Select Panorama > Managed Devices.</p>  If a user account is locked out, the Administrators page displays a lock in the Locked User column. You can click the lock to unlock the account.
Admin Roles	Enables you to define administrator roles, which involves defining the privileges and responsibilities of users who will access Panorama. Select Panorama > Managed Devices .
Access Domain	Enables you to control administrator access to device groups, templates, template stacks, and the web interface of firewalls. Select Panorama > Access Domains .
Authentication Profile	Enables you to specify a profile for authenticating access to Panorama. Select Device > Authentication Profile .
Authentication Sequence	Enables you to specify a series of authentication profiles to use for permitting access to Panorama. Select Device > Authentication Profile .

Panorama Page	Description
Managed Devices	Enables you to manage firewalls, which includes adding firewalls to Panorama as <i>managed devices</i> , displaying firewall connection and license status, tagging firewalls, updating firewall software and content, and loading configuration backups. See Panorama > Managed Devices .
Templates	Enables you to manage Panorama > Templates for the configuration options in the Device and Network tabs. Templates and template stacks enable you to reduce the administrative effort of deploying multiple firewalls with similar configurations.
Device Groups	Enables you to configure Panorama > VMware Service Manager , which group firewalls based on function, network segmentation, or geographic location. Device groups can include physical firewalls, virtual firewalls, and virtual systems. Typically, firewalls in a device group need similar policy configurations. Using the Policies and Objects tab on Panorama, device groups provide a way to implement a layered approach for managing policies across a network of managed firewalls. You can nest device groups in a tree hierarchy of up to four levels. Descendant groups automatically inherit the policies and objects of ancestor groups and of the Shared location.
Managed Collectors	Enables you to manage Panorama > Managed 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). A Panorama management server (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 <i>managed collectors</i> . You can also use this page to Install a Software Update on a Log Collector .  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 <code>request system system-mode [panorama logger]</code> . To view the current mode, run <code>show system info match system-mode</code> . A Dedicated Log Collector has no web interface, only a CLI. However, you can use the web interface of the Panorama management server to manage and configure Log Collectors.
Collector Groups	Enables you to Panorama > Collector Groups . A Collector Group logically groups up to 8 Log Collectors so you can apply the same configuration settings and assign firewalls to them. Panorama uniformly distributes the logs among all the disks in a Log Collector and across all members in the Collector Group. Each Panorama instance can have up to 16 Collector Groups.
VMware Service Manager	Enables you to Panorama > VMware Service Manager running on a VMware ESXi server by enabling communication between the NSX Manager and Panorama.
Certificate Management	Enables you to configure and manage certificates, certificate profiles, and keys. See Manage Firewall and Panorama Certificates .
Log Settings	Enables you to forward logs to Simple Network Management Protocol (SNMP) trap receivers, syslog servers, and email addresses.

Panorama Page	Description
Server Profiles	Enables you to configure profiles for the following server types that provide services to Panorama: <ul style="list-style-type: none"> • Device > Server Profiles > Email • Device > Server Profiles > SNMP Trap • Device > Server Profiles > Syslog • Device > Server Profiles > RADIUS • Device > Server Profiles > TACACS+ • Device > Server Profiles > LDAP • Device > Server Profiles > Kerberos
Scheduled Config Export	Enables you to Panorama > Device Deployment to a File Transfer Protocol (FTP) server or Secure Copy (SCP) server on a daily basis.
Software	Enables you to Panorama > Software .
Dynamic Updates	Enables 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. See Device > Dynamic Updates .
Support	Enables you to access product and security alerts from Palo Alto Networks. See Device > Support .
Device Deployment	Enables you to view and Panorama > Device Deployment .
Master Key and Diagnostics	Enables you to specify a master key to encrypt private keys on Panorama. Private keys are stored in encrypted form by default even if you don't specify a new master key. See Device > Master Key and Diagnostics .

Commit Your Changes in Panorama

Click **Commit** at the top right of the web interface to commit, validate, or preview your changes to the Panorama configuration or to the template, device group, and Collector Group configurations that Panorama pushes to firewalls and Log Collectors. Committing applies the candidate configuration to the running configuration, which activates all configuration changes since the last commit. Panorama queues commit operations so that you can initiate new commits while a previous commit is in progress. You can use the [Task Manager](#) () to clear the commit queue or see details about commits. For more information on configuration changes, commit processes, commit validations, and the commit queue, refer to [Panorama Commit and Validation Operations](#). To save, revert, import, export, or load configurations, see [Device > Setup > Operations](#).



As a best practice, commit changes to Panorama before committing changes to firewalls or Log Collectors.

Commit Setting	Description
Commit Type	Select one of the following: <ul style="list-style-type: none"> • Panorama—Commits the changes in the current candidate configuration to the running configuration on Panorama. • Template—Commits network and device configurations from Panorama templates or template stacks to firewalls. • Device Group—Commits policies and objects from Panorama device groups to firewalls or virtual systems. • Collector Group—Commits changes to the Log Collectors in Collector Groups.
Filters (Template and device group commits only)	Filter the list of templates, template stacks, or device groups and the associated firewalls and virtual systems.
Name (Template and device group commits only)	Select the templates, template stacks, device groups, firewalls, or virtual systems to which the commit applies.
Last Commit State (Template and device group commits only)	Indicates whether the firewall and virtual system configurations are currently synchronized with the template or device group configurations in Panorama.
HA Status (Template and device group commits only)	Indicates the high availability (HA) state of the listed firewalls: <ul style="list-style-type: none"> • Active—Normal traffic-handling operational state. • Passive—Normal backup state. • Initiating—The firewall is in this state for up to 60 seconds after bootup. • Non-functional—Error state. • Suspended—An administrator disabled the firewall. • Tentative—For a link or path monitoring event in an active/active configuration.

Commit Setting	Description
Preview Changes column (Template and device group commits only)	<p>Compares the candidate configuration to the running configuration with the results filtered to show only the settings for a specific template, template stack, device group, firewall, or virtual system.</p>  <p>Because the preview results display in a new window, your browser must allow pop-up windows. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-up windows.</p>
Select All (Template and device group commits only)	Selects every entry in the list.
Deselect All (Template and device group commits only)	Deselects every entry in the list.
Expand All (Template and device group commits only)	Displays only the templates, template stacks, or device groups, not the firewalls or virtual systems assigned to them.
Collapse All (Template and device group commits only)	Displays the firewalls or virtual systems assigned to templates, template stacks, or device groups.
Group HA Peers (Template and device group commits only)	<p>Select this option to group firewalls that are peers in a high availability (HA) configuration. The resulting list displays the active firewall (or active-primary firewall in an active/active configuration) first and displays the passive firewall (or active-secondary firewall in an active/active configuration) in parentheses. This enables you to easily identify firewalls that are in HA mode. When pushing shared policies, you can push to the grouped pair instead of individual peers.</p>  <p>For HA peers in an active/passive configuration, consider adding both firewalls or their virtual systems to the same device group, template, or template stack so that you can push the configuration to both peers simultaneously.</p>
Filter Selected (Template and device group commits only)	If you want the list to display only specific firewalls or virtual systems, select the firewalls and then select Filter Selected .
Merge with Candidate Config (Template and device group commits only)	<p>Select this option (selected by default) to merge and commit the Panorama configuration changes with any pending configuration changes that were implemented locally on the target firewall. If you clear this selection, the commit operation excludes the candidate configuration on the firewall.</p>  <p>Clear this selection if you allow firewall administrators to commit changes locally on a firewall and you don't want to include those local changes when committing changes from Panorama. Another best practice is to perform a configuration audit on the firewall to review any local changes before committing from Panorama.</p>

Commit Setting	Description
Include Device and Network Templates (Template and device group commits only)	Select this option (selected by default) to commit both device group and template changes to the selected firewalls and virtual systems in a single commit operation. To commit these changes as separate operations, clear this selection.
Force Template Values (Template and device group commits only)	Select this option (disabled by default) to override all local configuration and remove objects on the selected firewalls that don't exist in the template or template stack, or are overridden in the local configuration. The commit reverts all existing configuration on the firewall, and ensures that the firewall inherits only the settings defined in the template or template stack.
Description	<p>Enter a description (up to 512 characters) for the commit. A brief summary of what changed in the configuration is useful for informing other administrators who might want to know about the changes without performing a configuration audit.</p>  The System log for a commit event will truncate the description value if it exceeds the character limit for that log type.
Preview Changes (Panorama commits only)	<p>Click Preview Changes to 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 Device > Config Audit).</p>  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-up windows.
Validate Changes (Panorama, template, and device group commits only)	Select 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 Panorama or firewall configuration before committing the changes. The results display all the same errors and warnings displayed for a full commit, including rule shadowing and application dependency warnings, but the running configuration does not change. The validations help determine whether you can successfully commit your changes before attempting to commit, which reduces failures at commit time.
Commit	Click Commit to activate your changes. If another commit is in process, clicking Commit adds your request to the commit queue.

Defining Policies on Panorama

Device Groups on Panorama allow you to centrally manage policies on the 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 firewalls, 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 firewalls, 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 firewall. 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 firewall 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 Security Policy Rule](#)).

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

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

- [Policies > Security](#)
- [Policies > NAT](#)
- [Policies > QoS](#)
- [Policies > Policy Based Forwarding](#)
- [Policies > Decryption](#)
- [Policies > Application Override](#)
- [Policies > Captive Portal](#)
- [Policies > DoS Protection](#)

Logs and Reports on Panorama

The following table describes how log monitoring and report generation works in Panorama.

Panorama Log/Report	Description
Distributed log collection	Panorama performs two functions—configuration and log collection. To facilitate scalability in large deployments, you can use an M-Series appliance to separate the management and log collection functions. Configuring firewalls to send logs to an M-Series appliance in Log Collector mode (Dedicated Log Collector) helps offload the traffic-intensive log collection process from your Panorama management server (an M-Series appliance in Panorama mode or a Panorama virtual appliance). For details, refer to Centralized Logging and Reporting and Manage Log Collection .
Log forwarding	Panorama logs and reports provide information about user activity in the managed network. To view user and network activity on Panorama, you don't need to configure log forwarding from firewalls to Panorama. Log forwarding is required for long-term log storage and for generating reports using logs stored locally in Panorama. If you enable log forwarding , by default the firewalls buffer logs and send them at a predefined interval to Panorama, though you can change this setting (for details, see Device > Setup > Management).
Application Command Center (ACC)	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. For details, see ACC .
Report generation and scheduling	You can generate and schedule custom reports on Panorama. For scheduled predefined and custom reports, the firewalls aggregate report statistics every 15 minutes and forward them to Panorama on an hourly basis. For details, see Monitor > Manage Custom Reports .
Log and report management	<p>For details on the fields and tasks available for managing logs and reports, see:</p> <ul style="list-style-type: none"> • ACC • Monitor > Logs • Monitor > Logs • Monitor > PDF Reports > Manage PDF Summary • Monitor > PDF Reports > User Activity Report <p> On Panorama, you must set up a Master Device (firewall) for each device group to generate a User Activity report. You cannot generate Group Activity reports because Panorama does not have the information for mapping users to groups.</p>

Log Storage Partitions for a Panorama Virtual Appliance

▲ Panorama > Setup > Operations

By default, the Panorama virtual appliance has a single disk partition for all data in which 10.89GB is allocated for log storage; increasing disk size does not increase the log storage capacity. However, you can modify the log storage capacity using the following options:

- [Add another virtual disk](#). Panorama on VMware ESXi version 5.5 or later and on VMware vCloud Air can support a virtual disk of up to 8TB. Earlier ESXi versions support a virtual disk of up to 2TB.
- 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 271.
- 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 Panorama after changing the storage partition settings. Select **Panorama > Setup > Operations** and click **Reboot Panorama**.

The following table describes Panorama NFS V3 storage partition settings.

Panorama Storage Partition Setting—NFS V3	Description
Server	Specify the FQDN or IP address of the NFS server.
Log Directory	Specify the full path name of the directory where the logs will reside.
Protocol	Specify the protocol (UDP or TCP) for communication with the NFS server.
Port	Specify the port for communication with the NFS server.
Read Size	Specify the maximum size in bytes (range is 256–32,768) for NFS read operations.
Write Size	Specify the maximum size in bytes (range is 256–32,768) for NFS write operations.
Copy on Setup	Select this option 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.

Panorama > High Availability

To enable **high availability (HA)** on Panorama[■], configure the followings settings.

Panorama HA Setting	Description
Setup	
Click Edit () to configure the following settings.	
Enable HA	Select this option to enable HA.
Peer HA IP Address	Enter the IP address of the MGT interface on the peer.
Enable Encryption	<p>When enabled, the MGT interface encrypts communication between the HA peers. Before enabling encryption, export the HA key from each HA peer and import the key into the other peer. You perform key imports and exports on the Panorama > Certificate Management > Certificates page (see Manage Firewall and Panorama Certificates).</p> <p> HA connectivity uses TCP port 28 with encryption enabled and 28769 when encryption is not enabled.</p>
Monitor Hold Time (ms)	Enter the number of milliseconds that the system will wait before acting on a control link failure (range is 1,000–60,000; default is 3,000).
Election Settings	
Click Edit () to configure the following settings.	
Priority (Required on the Panorama virtual appliance)	<p>Assign one peer as Primary and the other as Secondary in the HA pair. This setting determines which peer is the primary recipient for firewall logs. When you Log Storage Partitions for a Panorama Virtual Appliance, you can use its internal disk (default) or a Network File System (NFS) for log storage. If you configure an NFS, only the primary recipient receives the firewall logs. If you configure internal disk storage, the firewalls send logs to both the primary and the secondary recipient by default, though you can change this by configuring the Logging and Reporting Settings.</p>
Preemptive	Select this option to enable the primary Panorama to resume active operation after recovering from a failure. If this setting is off, the secondary Panorama remains active even after the primary Panorama recovers from a failure.
HA Timer Settings	<p>Your selection determines the values for the remaining HA election settings, which control the failover speed:</p> <ul style="list-style-type: none"> • Recommended—Select this option for typical (default) failover timer settings. To see the associated values, select Advanced and Load Recommended. • Aggressive—Select this option for faster failover timer settings. To see the associated values, select Advanced and Load Aggressive. • Advanced—Selecting this option displays the remaining HA election settings so you can customize their values. <p>See the fields below for the Recommended and Aggressive values.</p>
Promotion Hold Time (ms)	Enter the number of milliseconds (range is 0–60,000) the secondary Panorama peer will wait before taking over after the primary peer goes down. The recommended (default) value is 2,000; the aggressive value is 500.

Panorama HA Setting	Description
Hello Interval (ms)	Enter the number of milliseconds (range is 8,000–60,000) between the hello packets sent to verify that the other peer is operational. The recommended (default) and aggressive value is 8,000.
Heartbeat Interval (ms)	Specify the frequency in milliseconds (range is 1,000–60,000) at which Panorama sends ICMP pings to the HA peer. The recommended (default) value is 2,000; the aggressive value is 1,000.
Preemption Hold Time (min)	This field applies only if you also select Preemptive . Enter the number of minutes (range is 1–60) the passive Panorama peer will wait before falling back to active status after it recovers from an event that caused failover. The recommended (default) and aggressive value is 1.
Monitor Fail Hold Up Time (ms)	Specify the number of milliseconds (range is 0–60,000) Panorama waits after a path monitor failure before attempting to re-enter the passive state. During this period, the passive peer is not available to take over for the active peer in the event of failure. This interval enables Panorama to avoid a failover due to the occasional flapping of neighboring devices. The recommended (default) and aggressive value is 0.
Additional Master Hold Up Time (ms)	Specify the number of milliseconds (range is 0–60,000) during which the preempting peer remains in the passive state before taking over as the active peer. The recommended (default) value is 7,000; the aggressive value is 5,000.

Path MonitoringClick Edit () to configure HA path monitoring .

Enabled	Select this option to enable path monitoring. Path monitoring enables Panorama to monitor specified destination IP addresses by sending ICMP ping messages to verify that they are responsive.
Failure Condition	Select whether a failover occurs when Any or All of the monitored path groups fail to respond.

Path GroupTo create a path group for HA path monitoring, click **Add** and complete the following fields.

Name	Specify a name for the path group.
Enabled	Select this option 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 the number of milliseconds between the ICMP echo messages that verify that the path to the destination IP address is up (range is 1,000–60,000; default is 5,000).
Ping Count	Specify the number of failed pings before declaring a failure (range is 3–10; default is 3).
Destination IPs	Enter one or more destination IP addresses to monitor. Use commas to separate multiple addresses.

Panorama > Administrators

Panorama administrative accounts define administrator [role and authentication parameters](#). To unlock a locked account, click the lock in the Locked User column. To create an administrator account, click **Add** and complete the following fields.

Administrator Account Setting	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. For details, see Device > Authentication Profile or Device > Authentication Sequence . You can use this setting for RADIUS, TACACS+, LDAP, Kerberos, or local database authentication .
Use only client certificate authentication (Web)	Select this option to use client certificate authentication for web access. If you select this option, a username (Name) and Password are not required; the certificate can 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. Device Group and Template administrators cannot access the Panorama > Administrators page. To change their local password, these administrators must click their username beside Logout at the bottom of the web interface. This also applies to administrators with a custom Panorama role in which access to the page is disabled. You can use password authentication in conjunction with an Authentication Profile (or sequence) or with local database authentication. You can set password expiration parameters by selecting a Password Profile (see Device > Password Profiles) and setting Minimum Password Complexity parameters (see Device > Setup > Management).
Use Public Key Authentication (SSH)	Select this option to use SSH public key authentication . Click Import Key and Browse to select the public key file. The 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).  If public key authentication fails, Panorama presents a login and password prompt.

Administrator Account Setting	Description
Administrator Type	<p>The type selection determines the administrative role  options:</p> <ul style="list-style-type: none"> • Dynamic—These roles provide access to Panorama and managed firewalls. When new features are added, Panorama automatically updates the definitions of dynamic roles; you never need to manually update them. • Custom Panorama Admin—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)	<p>Select a predefined role:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Create, modify, or delete Panorama or firewall administrators and roles. • Export, validate, revert, save, load, or import a configuration (Device > Setup > Operations). • Configure a Scheduled Config Export in the Panorama tab.
Profile (Custom Panorama Admin administrator type)	Select a custom Panorama role (see Panorama > Managed Devices).
Access Domain to Administrator Role (Device Group and Template Admin administrator type)	<p>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 Panorama > Access Domains), and then click the adjacent Admin Role cell and select a custom Device Group and Template administrator role from the drop-down (see Panorama > Managed Devices). 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. The Access Domain selection also filters the firewalls that the Context drop-down displays.</p> <p> If you use a RADIUS server to authenticate administrators, you must map administrator roles and access domains to RADIUS 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.</p>
Password Profile	Select a Password Profile (see Device > Password Profiles).

Panorama > Admin Roles

Admin Role profiles are custom roles that define the access privileges and responsibilities of administrators. For Device Group and Template administrators, you can map roles to access domains in an administrator account to enforce the separation of information among the functional or regional areas of your organization (for details, see [Panorama > Access Domains](#)).

To create an Admin Role profile, click **Add** and complete the following fields.



If you use a RADIUS server to authenticate administrators, [map the administrator roles and access domains to RADIUS Vendor Specific Attributes \(VSAs\)](#).

Panorama Administrator Role Setting	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.
Web UI	Select from the following options to set the type of access permitted for specific features in the Panorama context (Web UI list) and firewall context (Context Switch UI list): <ul style="list-style-type: none"> • Enable ()—Read and write access • Read Only ()—Read-only access • Disable ()—No access
XML API (Panorama role only)	Select the type of XML API access (Enable , Read Only , or Disable) for Panorama and managed firewalls: <ul style="list-style-type: none"> • Report—Access to Panorama and firewall reports. • Log—Access to Panorama and firewall logs. • Configuration—Permissions to retrieve or modify Panorama and firewall configurations. • Operational Requests—Permissions to run operational commands on Panorama and firewalls. • Commit—Permissions to commit Panorama and firewall configurations. • User-ID Agent—Access to the User-ID agent. • Export—Permissions to export files from Panorama and firewalls (such as configurations, block or response pages, certificates, and keys). • Import—Permissions to import files into Panorama and firewalls (such as software updates, content updates, licenses, configurations, certificates, block pages, and custom logs).

Panorama Administrator Role Setting	Description
Command Line (Panorama role only)	Select the type of role for CLI access: <ul style="list-style-type: none">• None—(Default) Access to the Panorama CLI not permitted.• superuser—Full access to Panorama.• superreader—Read-only access to Panorama.• panorama-admin—Full access to Panorama except for the following actions:<ul style="list-style-type: none">• Create, modify, or delete Panorama administrators and roles.• Export, validate, revert, save, load, or import a configuration.• Schedule configuration exports.

Panorama > Access Domains

Access domains  control the access that Device Group and Template administrators have to specific device groups (to manage policies and objects), templates (to manage network and device settings), and the web interface of managed firewalls (through context switching). You can define up to 4,000 access domains and manage them locally or using [RADIUS Vendor-Specific Attributes \(VSAs\)](#) . To create an access domain, click **Add** and complete the following fields.

Access Domain Setting	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	<p>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.</p> <ul style="list-style-type: none"> 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	<p>Enable or disable read-write access for specific device groups in the access domain. You can also click Enable All or Disable All. Enabling read-write access for a device group automatically enables the same access for its descendants. If you manually disable a descendant, access for its highest ancestor automatically changes to read-only. By default, access is disabled for all device groups.</p> <p>If you want the list to display only specific device groups, select the device group names and Filter Selected.</p>  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 (Corresponds to the Device/Virtual Systems column in the Access Domain page)	Select the firewalls to which the administrator can switch context for performing local configuration. If the list is long, you can filter by Device State , Platforms , Device Groups , Templates , Tags , and HA Status .

Panorama > Managed Devices

A Palo Alto Networks firewall that Panorama manages is called a managed device. 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 7.0 can manage firewalls running PAN-OS 7.0 or earlier supported versions, but cannot manage firewalls running PAN-OS 7.1.

- [Managed Firewall Administration](#)
- [Managed Firewall Information](#)
- [Firewall Software and Content Updates](#)
- [Firewall Backups](#)

Managed Firewall Administration

You can perform the following administrative tasks on firewalls.

Task	Description
Add	<p>Click Add and enter the firewall serial numbers (one per row) to add them as managed devices. The Managed Devices page will then display Managed Firewall Information, including connection status, installed updates, and properties that were set during initial configuration.</p> <p>After adding the firewalls, enable Panorama to manage them by entering the IP address of the Panorama management server on the firewalls (see Device > Setup > Management).</p>  The firewall registers with Panorama over an SSL connection with AES-256 encryption. Panorama and the firewall authenticate each other using 2,048-bit certificates and use the SSL connection for configuration management and log collection.
Delete	Select one or more firewalls and click Delete to remove them from the list of firewalls that Panorama manages.
Tag	Select one or more firewalls, click Tag , and enter a text string of up to 31 characters or select an existing tag. Do not use an empty space. Wherever the web interface displays a long list of firewalls (for example, in the dialog for installing software), tags provide one means to filter the list. For example, you can use a tag called branch office to filter for all branch office firewalls across your network.
Install	Click Install to install Firewall Software and Content Updates .
Group HA Peers	Select Group HA Peers if you want the Managed Devices page to group firewalls that are peers in a high availability (HA) configuration. You then can only select to perform actions on both peers or neither peer in each HA pair.
Manage (Backups)	Click Manage to manage Firewall Backups .

Managed Firewall Information

Select **Panorama > Managed Devices** to display the following information for each managed firewall.

Managed Firewall Information	Description
Device Group	<p>Displays the name of the Panorama > VMware Service Manager 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.</p> <p>Regardless of whether the column is visible, the page displays firewalls in clusters according to their device group. Each cluster has a header row that displays the device group name, the total number of assigned firewalls, the number of connected firewalls, and the device group path in the hierarchy. For example, 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.</p>
Device Name	<p>Displays the hostname or serial number of the firewall.</p> <p>For the VM-Series NSX edition firewall, the firewall name appends the hostname of the ESXi host. For example, PA-VM: Host-NY5105</p>
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 is assigned.

Managed Firewall Information	Description
Status	<p>Device State—Indicates the state of the connection between Panorama and the firewall—Connected or Disconnected. A VM-Series firewall can have two additional states:</p> <ul style="list-style-type: none"> • Deactivated—Indicates that you have deactivated a virtual machine either directly on the firewall or by selecting Deactivate VMs (Panorama > Device Deployment > Licenses) and removed all licenses and entitlements on the firewall. A deactivated firewall is no longer connected to Panorama because the deactivation process removes the serial number on the VM-Series firewall. • Partially deactivated—Indicates that you have initiated the license deactivation process from Panorama, but the process is not fully complete because the firewall is offline and Panorama cannot communicate with it.
	<p>HA Status—Indicates whether the firewall is:</p> <ul style="list-style-type: none"> • Active—Normal traffic-handling operational state • Passive—Normal backup state • Initiating—The firewall is in this state for up to 60 seconds after bootup • Non-functional—Error state • Suspended—An administrator disabled the firewall • Tentative—For a link or path monitoring event in an active/active configuration
	<p>Shared Policy—Indicates whether the policy and object configurations on the firewall are synchronized with Panorama.</p>
	<p>Template—Indicates whether the network and device configurations on the firewall are synchronized with Panorama.</p>
	<p>Last Commit State—Indicates whether the last commit failed or succeeded on the firewall.</p>
Software Version Apps and Threat Antivirus URL Filtering GlobalProtect Client WildFire	Displays the software and content versions that are currently installed on the firewall. For details, see Firewall Software and Content Updates .
Backups	On each firewall commit, PAN-OS automatically sends a firewall configuration backup to Panorama. Click Manage to view the available configuration backups and optionally load one. For details, see Firewall Backups .

Firewall Software and Content Updates

To install a software or content update on a managed firewall, first use the **Panorama > Device Deployment** pages to download or upload the update to Panorama. Then select the **Panorama > Managed Devices** page, click **Install**, and complete the following fields.



You can also install updates on firewalls using the **Panorama > Device Deployment** pages (see [Manage Software and Content Updates](#)).

Firewall Software/Content Update Installation Option	Description
Type	Select the type of update you want to install—PAN-OS Software , GlobalProtect Client software, Apps and Threats signatures, Antivirus signatures, WildFire , or URL Filtering .
File	Select the update image. The drop-down includes only images that you downloaded or uploaded to Panorama using the Panorama > Device Deployment pages.
Filters	Select Filters to filter the Devices list.
Devices	Select the firewalls on which you want to install the image.
Device Name	The firewall name.
Current Version	The update version of the selected Type that is currently installed on the firewall.
HA Status	Indicates whether the firewall is: <ul style="list-style-type: none"> • Active—Normal traffic-handling operational state • Passive—Normal backup state • Initiating—The firewall is in this state for up to 60 seconds after bootup • Non-functional—Error state • Suspended—An administrator disabled the firewall • Tentative—For a link or path monitoring event in an active/active configuration
Group HA Peers	Select this option if you want the Devices list to group firewalls that are peers in a high availability (HA) configuration.
Filter Selected	If you want the Devices list to display only specific firewalls, select the corresponding device names and Filter Selected .
Upload only to device	Select this option if you want to upload the image on the firewall, but don't want to automatically reboot the firewall. The image is installed when you manually reboot the firewall.
Reboot device after Install (Software only)	Select this option if you want to upload and install the software image. The installation process triggers a reboot.
Disable new apps in content update (Apps and Threats only)	Select this option if you want to disable applications in the update that are new relative to the last installed update. This protects against the latest threats while giving you the flexibility to enable applications after preparing any policy updates. Then, to enable applications, log in to the firewall, select Device > Dynamic Updates , click Apps in the Features column to display the new applications, and click Enable/Disable for each application you want to enable.

Firewall Backups

▲ Panorama > Managed Devices

Panorama automatically backs up every configuration change you commit to managed firewalls. To manage the backups for a firewall, select **Panorama > Managed Devices**, click **Manage** in the Backups column for the firewall, and perform any of the following tasks.



To configure the number of firewall configuration backups that Panorama stores, select **Panorama > Setup > Management**, edit the Logging and Reporting Settings, select **Log Export and Reporting**, and enter the **Number of Versions for Config Backups** (default is 100).

Task	Description
Display details about a saved or committed configuration.	In the Version column for the backup, click the saved configuration filename or committed configuration version number to display the contents of the associated XML file.
Restore a saved or committed configuration to the candidate configuration.	In the Action column for the backup, click Load and Commit .
Remove a saved configuration.	In the Action column for the saved backup, click Delete ().

Panorama > Templates

Through the **Device** and **Network** tabs, templates enable you to deploy a common base configuration to multiple firewalls that require similar settings. A template stack is a combination of templates. When managing firewall configurations with Panorama, you use a combination of device groups (to manage shared policies and objects) and templates (to manage shared device and network settings).

In addition to the fields displayed in the dialogs for creating [Templates](#) or [Template Stacks](#), the **Panorama > Templates** page displays the following columns:

- Type—Identifies the listed entries as templates or template stacks.
- Stack—Lists the templates assigned to a template stack.

The following topics provide additional information about templates and template stacks.

What do you want to do?	See:
Add, clone, edit, or delete a template	Templates
Add, clone, edit, or delete a template stack	Template Stacks
Looking for more?	Templates and Template Stacks
	Manage Templates and Template Stacks

Templates

To configure a template, click **Add** and complete the following fields.



After configuring a template, you must [Commit Your Changes in Panorama](#). After you [configure the network and device settings of firewalls assigned to the template](#), you must perform a template commit to push the settings to the firewalls.

Deleting a template, or removing a firewall from one, does not delete the values that Panorama has pushed to the firewall. When you remove a firewall from a template, Panorama no longer pushes new updates to the firewall.

Template Setting	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 if you want Panorama to push configurations that are specific to that virtual system (for example, interfaces) to firewalls that don't have multiple virtual systems.
Description	Enter a description for the template.

Template Setting	Description
Devices	<p>Select each firewall that you want to add to the template. You can assign a given firewall to only one template or stack. Therefore, if you will use the template only within a stack, do not assign firewalls to the template, just to the stack (see Template Stacks).</p> <p>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.</p>  You can assign firewalls that have non-matching modes (VPN mode, multiple virtual systems mode, or operational mode) to the same template. Panorama pushes mode-specific settings only to firewalls that support those modes.
Select All	Selects every firewall in the list.
Deselect All	Deselects every firewall in the list.
Group HA Peers	<p>Select this option to group firewalls that are high availability (HA) peers. The list then displays the active firewall (or active-primary firewall in an active/active configuration) first and displays the passive firewall (or active-secondary firewall in an active/active configuration) in parentheses. This option enables you to easily identify firewalls that have an HA configuration and, when pushing template settings, you can push to the grouped pair instead of to each firewall individually.</p>
Filter Selected	To display only specific firewalls, select the firewalls and then Filter Selected .

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. To configure a template stack, click **Add Stack** and complete the following fields.



After configuring a template stack, you must [Commit Your Changes in Panorama](#). After you [configure the network and device settings of firewalls assigned to the stack](#), you must perform a template commit to push the settings to the firewalls.

Deleting a template stack, or removing a firewall from one, does not delete the values that Panorama has pushed to the firewall. When you remove a firewall from a template stack, Panorama no longer pushes new updates to the firewall.

Template Stack Setting	Description
Name	<p>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.</p> <p>In the Device and Network tabs, the Template drop-down will display the stack name and its assigned templates.</p>
Description	Enter a description for the stack.
Templates	<p>For each template you want to include in the stack (up to 16), click Add and select the template.</p> <p>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.</p> <p> Panorama doesn't validate template combinations in stacks, so plan the order in a way that avoids invalid relationships.</p>
Devices	<p>Select each firewall that you want to add to the stack.</p> <p>If the list of firewalls is long, you can filter it by Platforms, Device Groups, Tags, and HA Status.</p> <p> You can assign firewalls that have non-matching modes (VPN mode, multiple virtual systems mode, or operational mode) to the same stack. Panorama pushes mode-specific settings only to firewalls that support those modes.</p>
Select All	Selects every firewall in the list.
Deselect All	Deselects every firewall in the list.
Group HA Peers	Select this option 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 from the template stack, you can push to the grouped pair instead of to each firewall individually.
Filter Selected	To display only specific firewalls, select the firewalls and then Filter Selected .

Panorama > Device Groups

Device groups comprise firewalls and virtual systems you want to manage as a group, such as 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 under the Shared location 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*. In the **Device Groups** page, the Name column reflects this hierarchy.

After adding, editing, or deleting a device group, you must perform both a Panorama and device group commit (see [Commit Your Changes in Panorama](#)). Panorama then pushes configuration changes to firewalls assigned to the device group. To configure a device group, click **Add** and complete the following fields.

Device Group Setting	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 each firewall that you want to add to the device group. If the list of firewalls is long, you can filter by Device State , Platforms , Templates , or Tags . The Filters section displays (in parentheses) the number of managed firewalls for each of these categories. If the purpose of a device group is purely organizational (that is, to contain other device groups), you don't need to assign firewalls to it.
Select All	Selects every firewall and virtual system in the list.
Deselect All	Deselects every firewall and virtual system in the list.
Group HA Peers	Select this option 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 firewalls and then Filter Selected .
Parent Device Group	Relative to the device group you are defining, select the device group (or the Shared location) that is just above it in the hierarchy (default is Shared).
Master Device	Select the one firewall in the device group from which Panorama will collect User-ID™ information for use in policies. The collected user and group mapping information is specific to the device group.

Panorama > Managed Collectors

An M-Series appliance in Panorama mode and a Panorama virtual appliance can both manage Dedicated Log Collectors (M-Series appliances in Log Collector mode). An M-Series appliance in Panorama mode also has a default (local) Log Collector to process the logs it receives directly from firewalls. (A Panorama virtual appliance processes the logs it receives directly from firewalls without using a local Log Collector.) To use Panorama for managing a Dedicated Log Collector, you must add it as a *managed collector*. The predefined managed collector named default is local to the M-Series appliance in Panorama mode.

What do you want to do?	See:
Display Log Collector information	View Log Collector Information
Add, edit, or delete a Log Collector	Configure a Log Collector
Update Panorama software on a Log Collector	Install a Software Update on a Log Collector
Looking for more?	Centralized Logging and Reporting  Configure a Managed Collector 

View Log Collector Information

Select **Panorama > Managed Collectors** to display the following information for Log Collectors. Additional parameters are visible when you [Configure a Log Collector](#).

Log Collector Information	Description
Collector Name	The name that identifies this Log Collector. This name displays as the Log Collector hostname.
Collector Serial Number	The serial number of the M-Series appliance that functions as the Log Collector.
Software Version	The Panorama software release installed on the Log Collector.
IP Address	The IP address of the management interface on the Log Collector.
Connected	The status of the connection between the Log Collector and Panorama.
Configuration Status/Detail	Indicates whether the configuration on the Log Collector is synchronized with Panorama.
Run Time Status/Detail	The status of the connection between this and other Log Collectors in the Collector Group.
Redistribution State	Certain actions (for example, adding disks) will cause the Log Collector to redistribute the logs among its disk pairs. This column indicates the completion status of the redistribution process as a percentage.
Last Commit State	Indicates whether the last Collector Group commit performed on the Log Collector failed or succeeded.

Log Collector Information	Description
Statistics	After you Configure a Log Collector , click Statistics to view disk information, CPU performance, and the average log rate (logs/second). To better understand the log range you are reviewing, you can also view information on the oldest log that the Log Collector received.

Configure a Log Collector

To [configure a Log Collector](#), click **Add** and define the settings as follows.

What do you want to know?	See:
Identify the Log Collector and define its connections to the Panorama management server, DNS servers, and NTP servers.	Define General Log Collector Settings
Configure access to the Log Collector CLI.	Define Log Collector CLI Authentication Settings
Configure the interfaces that the Log Collector uses.	Define Log Collector Management, Eth1, and Eth2 Interface Settings
Configure the RAID disks that store logs collected from firewalls.	Define Log Collector RAID Disk Settings

Define General Log Collector Settings

▲ Panorama > Managed Collectors > General

Complete the following field to identify a Log Collector and define its connections to the Panorama management server, DNS servers, and NTP servers.

Log Collector General Setting	Description
Collector S/N	Enter the serial number of the M-Series appliance that functions as the Log Collector. This field is required.
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 Log Collector hostname.
Device Log Collection	Select the interface to use for firewall log collection. By default, the management (MGT) interface performs this function. To select Eth1 or Eth2, you must first enable those interfaces on the Panorama management server (for details, see Device > Setup > Management , Eth1/Eth2 Interface Settings).
Collector Group Communication	Select the interface to use for communication within Collector Groups. By default, the MGT interface performs this function. To select Eth1 or Eth2, you must first enable those interfaces on the Panorama management server (for details, see Device > Setup > Management , 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 Manage Firewall and Panorama Certificates). When you assign a Syslog server profile to the Collector Group that includes this Log Collector (see Panorama > Collector Groups , Panorama > Collector Groups > Collector Log Forwarding), the Transport protocol of the server profile must be SSL (see Device > Server Profiles > Syslog).
Panorama Server IP	Specify the IP address of the Panorama management server that manages this Log Collector.
Panorama Server IP 2	Specify the IP address of the secondary peer if the Panorama management server is deployed in a high availability (HA) configuration.
Domain	Enter the domain name of the Log Collector.
Primary DNS Server	Enter the IP address of the primary DNS server. The Log Collector uses this server for DNS queries (for example, to find the Panorama management server).
Secondary DNS Server	(Optional) Enter the IP address a secondary DNS server to use if the primary server is unavailable.

Log Collector General Setting	Description
Primary NTP Server	Enter the IP address or host name of the primary NTP server, if any. If you do not use NTP servers, you can set the Log Collector time manually.
Secondary NTP Server	(Optional) Enter the IP address or host name of secondary NTP servers to use if the primary server is unavailable.
Timezone	Select the time zone of the Log Collector.
Latitude	Enter the latitude (-90.0 to 90.0) of the Log Collector. Traffic and threat maps use the latitude for App Scope.
Longitude	Enter the longitude (-180.0 to 180.0) of the Log Collector. Traffic and threat maps use the longitude for App Scope.

Define Log Collector CLI Authentication Settings

▲ Panorama > Managed Collectors > Authentication

An M-Series appliance in Log Collector mode (Dedicated Log Collector) has no web interface, only a CLI. You can use an M-Series appliance in Panorama mode to configure most settings on a Dedicated Log Collector but some settings require CLI access. To configure authentication settings for CLI access, configure the following fields.

Log Collector Authentication Setting	Description
Users	This field will always show <code>admin</code> and is used for the local CLI login name on the Log Collector.
Mode	Select the password Mode : <ul style="list-style-type: none"> • Password—Enter a plaintext Password and Confirm Password. • Password Hash—Enter a hashed password string. This can be useful if, for example, you want to reuse the password of an existing Unix account but do not know the plaintext password, only the hashed password. Panorama accepts any string of up to 63 characters regardless of the algorithm used to generate the hash value. The operational CLI command <code>request password-hash password <password></code> uses the MD5 algorithm. When you commit your changes, Panorama pushes the hash value to the Log Collector and the administrator password will be the specified <code><password></code>.
Failed Attempts	Enter the number of failed login attempts (1-10) that are allowed for the CLI before locking out the administrator account. The default 0 specifies unlimited login attempts. Limiting login attempts can help protect the Log Collector from brute force attacks.  If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, the Failed Attempts is ignored and the user is never locked out. If you use the default 0 for both fields, the user is never locked out.
Lockout Time	Enter the number of minutes (0-60) for which the Log Collector locks out the administrator out after reaching the number of Failed Attempts .  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. If you use the default 0 for both fields, the user is never locked out.

Define Log Collector Management, Eth1, and Eth2 Interface Settings

▲ Panorama > Managed Collectors > Management/Eth1/Eth2

Log Collectors use the **Management** (MGT) interface for management and configuration traffic. By default, Log Collectors also use MGT for log collection and communication within Collector Groups, though you can assign those functions to the Ethernet 1 (**Eth1**) and Ethernet 2 (**Eth2**) interfaces. If you assign **Eth1** or **Eth2**, it is a best practice to define a separate subnet for the MGT interface that is more private than the Eth1 or Eth2 subnets. **Eth1** and **Eth2** are available only if you configured them for the Panorama management server (see [Device > Setup > Management](#)).

To configure the interfaces, complete the fields in the **Management**, **Eth1**, and **Eth2** tabs.



To complete the configuration of the MGT interface, you must specify the IP address, netmask or prefix length, 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 through the console port for future configuration changes. It is recommended that you commit a complete configuration.

You cannot commit the Eth1 or Eth2 configuration unless you specify the IP address, netmask or prefix length, and default gateway.

Log Collector Management, Eth1, or Eth2 Interface Setting	Description
Eth1 / Eth2 (Eth1 and Eth2 interfaces only)	Select this option to enable the interface. The MGT interface is enabled by default.
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	Assign an IPv4 address to the interface if your network uses IPv4.
Netmask	Enter a network mask (for example, 255.255.255.0) if you assigned an IPv4 address to the interface.
Default Gateway	Assign an IPv4 address to the default router if the interface has an IPv4 address. The router and interface must be on the same subnet.
IPv6 Address/Prefix Length	Assign an IPv6 address to the interface if your network uses IPv6. To indicate the netmask, enter an IPv6 prefix length (for example, 2001:400:f00::1/64).
IPv6 Default Gateway	Assign an the IPv6 address to the default router if the interface has an IPv6 address. The router and interface must be on the same subnet.
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range is 576–1,500; default is 1,500).
SSH (MGT interface only)	Select this option to enable SSH on the MGT interface.
SNMP (MGT interface only)	Select this option to enable Simple Network Managed Protocol (SNMP) on the MGT interface. This is required to use SNMP to monitor Log Collector statistics.
Ping	Select this option to enable Ping on the interface.
Permitted IP Addresses	Add the IP addresses from which administrators can manage this interface. By default, if you don't add any, administrators can use any IP address.

Define Log Collector RAID Disk Settings

▲ Panorama > Managed Collectors > Disks

To increase log storage capacity , Add one or more disk pairs.

By default, the M-Series appliance is shipped with the first RAID 1 disk pair enabled and installed in bays A1/A2. You can add up to three more disk pairs in bays B1/B2, C1/C2, and D1/D2. In the software, the disk pair in bays A1/A2 is named Disk Pair A.

After you add disk pairs, the Log Collector redistributes its existing logs across all the disks, which can take hours for each terabyte of logs. During the redistribution process, the maximum logging rate is reduced. In the **Panorama > Managed Collectors** page, the Redistribution State column indicates the completion status of the process as a percentage.

Install a Software Update on a Log Collector

▲ Panorama > Managed Collectors

To install a software image on a an M-Series appliance in Log Collector mode, download or upload the image to Panorama (see [Panorama > Device Deployment](#)), click **Install** and complete the following fields.



You can also use the **Panorama > Device Deployment > Software** pages to install updates on Log Collectors (see [Manage Software and Content Updates](#)).

Field for Installing a Software Update on a Log Collector	Description
File	Select a downloaded or uploaded software image.
Devices	Select the Log Collectors on which to install the software. The dialog displays the following information for each Log Collector: <ul style="list-style-type: none"> Device Name—The name of the M-Series appliance in Log Collector mode. Current Version—The Panorama software release currently installed on the Log Collector. HA Status—This column does not apply to Log Collectors. Dedicated Log Collectors do not support high availability.
Filter Selected	To display only specific Log Collectors, select the Log Collectors and Filter Selected .
Upload only to device (do not Install)	Select this option to upload the software to the Log Collector without automatically rebooting it. The image is not installed until you manually reboot by logging into the Log Collector CLI and running the <code>request restart system</code> operational command.
Reboot device after Install	Select this option to upload and automatically install the software. The installation process reboots the Log Collector.

Panorama > Collector Groups

Each Collector Group can have up to 16 Log Collectors, to which you assign firewalls for forwarding logs. You can then use Panorama to query the Log Collectors for aggregated log viewing and investigation.



The predefined Collector Group named default contains the predefined Log Collector that is local to the M-Series appliance in Panorama mode.

- [Configure a Collector Group](#)
- [View Collector Group Information](#)

Configure a Collector Group

To [configure a Collector Group](#), click **Add** and complete the following fields.

Collector Group Setting	Configured In	Description
Name	Panorama > Collector Groups > General	Enter a name to identify this Collector Group (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Log Storage		<p>Indicates the current storage quota for firewall logs that the Collector Group receives.</p> <p>Select this option to set the storage Quota and expiration period (Max Days) for each log type and extended threat PCAPs. For details on quotas and expiration periods, see Device > Setup > Management, Logging and Reporting Settings.</p> <p>To use the default settings, click Restore Defaults.</p>
Min Retention Period (days)		Enter the minimum log retention period in days (1-2,000) that Panorama maintains across all Log Collectors in the Collector Group. If the current date minus the date of the oldest log is less than the defined minimum retention period, Panorama generates a System log as an alert violation.
Enable log redundancy across collectors		<p>If you select this option, each log in the Collector Group will have two copies and each copy will reside on a different Log Collector. This redundancy ensures that, if any one Log Collector becomes unavailable, no logs are lost—you can see all the logs forwarded to the Collector Group and run reports for all the log data. Log redundancy is available only if the Collector Group has multiple Log Collectors and each Log Collector has the same number of disks.</p> <p>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).</p> <p> Because enabling redundancy creates more logs, this configuration requires more storage capacity. Enabling redundancy doubles the log processing traffic in a Collector Group, which reduces its maximum logging rate by half, as each Log Collector must distribute a copy of each log it receives. (When a Collector Group runs out of space, it deletes older logs.)</p>

Collector Group Setting	Configured In	Description
Location	Panorama > Collector Groups > Monitoring	Specify the location of the M-Series appliance in Log Collector mode.
Contact		Specify an email contact (for example, the email address of the SNMP administrator who will monitor the Log Collectors).
Version		<p>Specify the SNMP version for communication with the Panorama management server—V2c or V3.</p> <p>SNMP enables you to collect information about Log Collectors, including connection status, disk drive statistics, software version, average CPU usage, average logs/second, and storage duration per log type. SNMP information is available on a per Collector Group basis.</p>
SNMP Community String (V2c only)		<p>Enter the SNMP Community String, which identifies a community of SNMP managers and monitored devices (Log Collectors, in this case), and serves as a password to authenticate the community members to each other.</p> <p> Don't use the default community string public; it is well known and therefore not secure.</p>
Views (V3 only)		<p>Add a group of SNMP views and, in Views, enter a name for the group. Each view is a paired object identifier (OID) and bitwise mask—the OID specifies a managed information base (MIB) and the mask (in hexadecimal format) specifies which SNMP objects are accessible within (include matching) or outside (exclude matching) that MIB.</p> <p>For each view in the group, Add the following settings:</p> <ul style="list-style-type: none"> • View—Enter a name for a view. • OID—Enter the OID. • Option (include or exclude)—Choose whether the view will exclude or include the OID. • Mask—Specify a mask value for a filter on the OID (for example, 0xf0).
Users (V3 only)		<p>Add the following settings for each SNMP user:</p> <ul style="list-style-type: none"> • Users—Enter a username for authenticating the user to the SNMP manager. • View—Select a group of views for the user. • Authpwd—Enter a password for authenticating the user to the SNMP manager (minimum eight characters). Only Secure Hash Algorithm (SHA) is supported for encrypting the password. • Privpwd—Enter a privacy password for encrypting SNMP messages to the SNMP manager (minimum eight characters). Only Advanced Encryption Standard (AES) is supported.

Collector Group Setting	Configured In	Description
Collector Group Members	Panorama > Collector Groups > Device Log Forwarding	<p>Click Add and, from the drop-down, select the Log Collectors that will be part of this Collector Group (up to 16). The drop-down will show all Log Collectors that are available in the Panorama > Managed Collectors page. All the Log Collectors for any particular Collector Group must be the same platform (all M-100 appliances or all M-500 appliances).</p>  <p>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.</p>
Devices		<p>You must add Collector Group Members (Log Collectors) before you can add firewalls to the Collector Group.</p> <p>To add firewalls, click Add, click Modify in the Devices list, select the managed firewalls, and 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 Move Up or Move Down. After assigning all the Log Collectors in the desired order, click OK.</p>
System	Panorama > Collector Groups > Collector Log Forwarding	Select the firewall logs that you want forward from this Collector Group to external servers (SNMP Trap, Email, or Syslog).
Config		To configure server profiles for these destinations, see Device > Server Profiles > SNMP Trap , Device > Server Profiles > Syslog , and Device > Server Profiles > Email .
HIP Match		
Traffic		
Threat		
WildFire		
Correlation		 A PA-7000 Series firewall cannot forward logs to Panorama; you must forward the logs directly  from the firewall to external servers.

View Collector Group Information

Select **Panorama > Collector Groups** to display the following information for Collector Groups. Additional fields are visible when you [Configure a Collector Group](#).

Collector Group Information	Description
Name	A name that identifies the Collector Group.
Redundancy Enabled	Indicates whether log redundancy is enabled for the Collector Group. You can enable log redundancy for a collector group when you modify or Configure a Collector Group .
Collectors	The Log Collectors assigned to the Collector Group.
Redistribution State	Certain actions (for example, enabling log redundancy) will cause the Collector Group to redistribute the logs among its Log Collectors. This column indicates the completion status of the redistribution process as a percentage.

Panorama > VMware Service Manager

To automate the provisioning of a VM-Series NSX edition firewall, you must enable communication between the NSX Manager and Panorama. When Panorama registers the VM-Series firewall as a service on the NSX Manager, the NSX Manager has the configuration settings required to provision one or more instances of the VM-Series firewalls on each ESXi host in the cluster.

What do you want to know?	See:
How do I configure Panorama to communicate with the NSX Manager?	Configure Access to the NSX Manager
How do I define the configuration for the VM-Series NSX edition firewall?	Create Service Definitions
How do I configure the firewall to consistently enforce policy in the dynamic vSphere environment?	Select Objects > Address Groups and Policies > Security . To enable Panorama and the firewalls to learn about the changes in the virtual environment, use Dynamic Address Groups as source and destination address objects in security policy pre rules.
Looking for more?	See Set up a VM-Series NSX Edition Firewall .

Configure Access to the NSX Manager

- ▲ [VMware Service Manager Settings](#)
- ▲ [VMware Service Manager Connection Status](#)

VMware Service Manager Settings

To enable Panorama to communicate with the NSX Manager, click **Edit** () and complete the following fields.

VMware Service Manager Settings	Description
Service Manager Name	Enter a name to identify the VM-Series firewall as a service. This name displays on the NSX Manager and is used to deploy the VM-Series firewall on-demand. Supports up to 63 characters; use only letters, numbers, hyphens, and underscores.
Description	(Optional) Enter a label to describe the purpose or function of this service.
NSX Manager URL	Specify the URL that Panorama will use to establish a connection with the NSX Manager.
NSX Manager Login	Enter the authentication credentials—username and password—configured on the NSX Manager. Panorama uses these credentials to authenticate with the NSX Manager.
NSX Manager Password	
Confirm NSX Manager Password	 The ampersand (&) special character is not supported in the NSX manager account password. If a password includes an ampersand, the connection between Panorama and NSX manager fails.

VMware Service Manager Connection Status

After committing the changes to Panorama, the VMware Service Manager page displays the connection status between Panorama and the NSX Manager.

Type	Description
Status	<p>Displays the connection status between Panorama and the NSX Manager. A successful connection displays as Registered—Panorama and the NSX Manager are synchronized and the VM-Series firewall is registered as a service on the NSX Manager.</p> <p>For an unsuccessful connection, the status can be:</p> <ul style="list-style-type: none"> • Connected Error—Unable to reach/establish a network connection with the NSX Manager. • Not authorized—The access credentials (username and/or password) are incorrect. • Unregistered—The service manager, service definition, or service profile is unavailable or was deleted on the NSX Manager. • Out of sync—The configuration settings defined on Panorama are different from what is defined on the NSX Manager. Click Out of sync for details on the reasons for failure. For example, NSX Manager may have a service definition with the same name as defined on Panorama. To fix the error, use the service definition name listed in the error message to validate the service definition on the NSX Manager. Until the configuration on Panorama and the NSX Manager is synchronized, you cannot add a new service definition on Panorama.
Last Dynamic Update	Displays the date and time when Panorama retrieved the Dynamic Address Group information from the NSX Manager.

Synchronize Panorama with the NSX Manager

Use the **VMware Service Manager** page to perform the following operations.

Task	Description
NSX Config-Sync	<p>Click NSX Config-Sync to synchronize the service definitions configured on Panorama with the NSX Manager. If you have any pending commits on Panorama, this option is not available.</p> <p>If the synchronization fails, view the details in the error message to know whether the error is on Panorama or on the NSX Manager. For example, when you delete a service definition on Panorama, the synchronization with the NSX Manager fails if the service definition is referenced in a rule on the NSX Manager. Use the information in the error message to determine the reason for failure and where you need to take corrective action (on Panorama or on the NSX Manager).</p>
Synchronize Dynamic Objects	<p>Click Synchronize Dynamic Objects to refresh the dynamic object information from the NSX Manager. Synchronizing dynamic objects enables you to maintain context on changes in the virtual environment and allows you to safely enable applications by automatically updating the Dynamic Address Groups used in policy rules.</p> <p> On Panorama, you can view only the IP addresses that are dynamically registered from the NSX Manager. Panorama does not display the dynamic IP addresses that are registered directly to the firewalls. If you use VM Information Sources (not supported on the VM-Series NSX edition firewalls) or the XML API to register IP addresses dynamically to the firewalls, you must log in to each firewall to view the complete list of dynamic IP addresses (both those that Panorama pushed and those that are locally registered) on the firewall.</p>
Remove VMware Service Manager	<p>Click Remove VMware Service Manager to delete access to the NSX Manager and disable communication between Panorama and the NSX Manager.</p> <p> Before you remove the service manager configuration, you must first delete all service definitions.</p>

Create Service Definitions

A service definition allows you to register the VM-Series firewall as a partner security service on the NSX Manager. You can define up to 32 service definitions on Panorama and synchronize them on the NSX Manager.

Typically, you will create one service definition for each tenant in an ESXi cluster. Each service definition specifies the OVF (PAN-OS version) used to deploy the firewall and includes the configuration for the VM-Series firewalls installed on the ESXi cluster. To specify the configuration, a service definition must have a unique template, a unique device group and the license auth-codes for the firewalls that will be deployed using the service definition. When the firewall is deployed, it connects to Panorama and receives both its configuration settings—including the zone(s) for each tenant or department that the firewall will secure—and its policy settings from the device group specified in the service definition.

To add a new service definition, fill in the following fields.

Field	Description
Name	Enter the name for the service you want to display on the NSX Manager.
Description	(Optional) Enter a label to describe the purpose or function of this service definition.
Template	Select the template to which the VM-Series firewalls will be assigned. For details, see Panorama > Templates . Each service definition must be assigned to a unique template or template stack. A template can have multiple zones (NSX Service Profile Zones for NSX) associated with it. For a single-tenant deployment, create one zone (NSX Service Profile Zone) in the template. If you have a multi-tenant deployment, create a zone for each sub-tenant. When you create a new NSX Service Profile Zone, it is automatically attached to a pair of virtual wire subinterfaces. For more information, see Network > Zones .
VM-Series OVF URL	Enter the URL (IP address or host name and path) where the NSX Manager can access the OVF file to provision new VM-Series firewalls.
Authorization Code	Enter the authorization code from the order fulfillment email you received when you purchased the VM-Series firewall.
Device Group	Select the device group or device group hierarchy to which these VM-Series firewalls will be assigned. For details, see Panorama > VMware Service Manager .

Field	Description
Notify Device Groups	<p>Add the device groups that must be notified of additions or modifications to the virtual machines deployed on the network. As new virtual machines are provisioned or existing machines are modified, the changes in the virtual network are provided as updates to Panorama. When configured to do so, Panorama populates and updates the dynamic address objects referenced in policy rules so that the firewalls in the specified device groups receive changes to the registered IP addresses in the dynamic address groups.</p> <p> To enable notification, make sure to select every device group to which you want to enable notification. If you are not able to select a device group (no check box available), it means that the device group is automatically included by virtue of the device group hierarchy.</p> <p>This notification process creates context awareness and maintains application security on the network. If, for example, you have a group of hardware-based perimeter firewalls that must be notified when a new application or web server is deployed, this process initiates an automatic refresh of the dynamic address groups for the specified device group. And all policy rules that reference the dynamic address object now automatically include any newly deployed or modified application or web servers and can be securely enabled based on your criteria.</p>

Panorama > Log Settings

Panorama can aggregate firewall and managed collector logs and forward them as SNMP traps, syslog messages, or email notifications to the destinations you select. Before starting, you must define server profiles for the destinations (see [Device > Server Profiles > SNMP Trap](#), [Device > Server Profiles > Syslog](#), and [Device > Server Profiles > Email](#)).

On a Panorama virtual appliance, use the **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 page to [enable forwarding of the logs that Panorama and Log Collectors](#) generate, but “Configure a Collector Group” to enable forwarding of firewall logs.

The following table describes the logs and forwarding options on the **Log Settings** page.



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.

Log Settings Section	Description
System	To enable log forwarding for a particular severity level, click that level in the Severity column and select the desired server profiles. The severity indicates the urgency and impact of the system event: <ul style="list-style-type: none">• 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.

Log Settings Section	Description
Correlation	<p>Correlation logs are created when the definition for a correlation object matches traffic patterns on your network. For information on correlation objects, see Monitor > Automated Correlation Engine.</p> <p>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 that level in the Severity column and select the desired server profiles.</p> <p>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:</p> <ul style="list-style-type: none"> • 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.
Threat	<p>To enable log forwarding for a particular severity level, click that level in the Severity column and select the desired server profiles. The severity indicates the urgency and impact of the threat:</p> <ul style="list-style-type: none"> • 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.

Log Settings Section	Description
Config	Config logs record all changes to the firewall or Panorama configuration. To enable forwarding, edit Config settings 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, edit the HIP Match settings 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, edit the Traffic settings and select the desired server profiles.
WildFire	WildFire scans files and assigns a verdict. To enable log forwarding for a particular verdict, click that verdict in the Verdict column and select the desired server profiles. The verdicts are: <ul style="list-style-type: none">• 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.

Panorama > Scheduled Config Export

To schedule an [export of all the running configurations](#) on Panorama and firewalls, click **Add** and complete the following fields.



If Panorama has a high availability (HA) configuration, you must perform these instructions on each peer to ensure the scheduled exports continue after a failover. Panorama does not synchronize scheduled configuration exports between HA peers.

Scheduled Configuration Export Setting	Description
Name	Enter a name to identify the configuration export job (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.
Description	Enter an optional description.
Enable	Select this option to enable the export job.
Scheduled export start time (daily)	Specify the time of day to start the export (24 hour clock, format HH:MM).
Protocol	Select the protocol to use to export logs from Panorama to a remote host. Secure Copy (SCP) is a secure protocol; FTP is not.
Hostname	Enter the IP address or hostname of the target SCP or FTP server.
Port	Enter the port number on the target server.
Path	Specify the path to the folder or directory on the target server that will store the exported configuration. For example, if the configuration bundle is stored in a folder called <code>exported_config</code> within a top level folder called <code>Panorama</code> , the syntax for each server type is: <ul style="list-style-type: none"> • SCP server: <code>/Panorama/exported_config</code> • FTP server: <code>//Panorama/exported_config</code>
Enable FTP Passive Mode	Select this option to use FTP passive mode.
Username	Specify the username required to access the target system.
Password / Confirm Password	Specify the password required to access the target system.
Test SCP server connection	Select this option to test communication between Panorama and the SCP host/server. To enable the secure transfer of data, you must verify and accept the host key of the SCP server. The connection is not established until the host key is accepted. If Panorama has an HA configuration, you must perform this verification on each HA peer so that each one accepts the host key of the SCP server.

Panorama > Software

Use this page to manage Panorama software updates on the Panorama management server.

- [Manage Panorama Software Updates](#)
- [Display Panorama Software Update Information](#)

Manage Panorama Software Updates

Select **Panorama > Software** to perform the following tasks.



By default, the Panorama management server saves up to two software updates. To make space for newer updates, the server automatically deletes the oldest update. You can [change the number of software images that Panorama saves](#) and manually delete images to free up space.

Refer to [Install Content and Software Updates for Panorama](#) for important information about version compatibility.

Task	Description
Check Now	If Panorama has access to the Internet, click Check Now to display the latest update information (see Display Panorama Software Update Information). If Panorama does not have access to the external network, use a browser to visit the Software Update site for update information.
Upload	To upload a software image when Panorama does not have access to the Internet, use a browser to visit the Software Update site, locate the desired release and download the software image to a computer that Panorama can access, click Upload in the Panorama > Software page, Browse to the software image, and click OK . When the upload is complete, the Available column displays Uploaded.
Download	If Panorama has access to the Internet, click Download in the Action column for the desired release. When the download is complete, the Available column displays Downloaded.
Install	Click Install in the Action column to install the software image. When the installation finishes, Panorama logs you out while it reboots.  Panorama periodically performs a file system integrity check (FSCK) to prevent corruption of the Panorama system files. This check occurs after eight reboots or at a reboot that occurs 90 days after the last FSCK. A warning appears in the web interface and SSH login screens if an FSCK is in progress and you cannot log in until it completes. The time to complete this process varies by storage system size; for a large system, it can take several hours before you can log back into Panorama. To view progress, set up console access to Panorama.
Release Notes	If Panorama has access to the Internet, click Release Notes to access the release notes for the desired software release and review the release changes, fixes, known issues, compatibility issues, and changes in default behavior. If Panorama does not have access to the Internet, use a browser to visit the Software Update site and download the appropriate release.

Task	Description
<input checked="" type="checkbox"/>	Deletes a software image when no longer needed or when you want to free up space for more images.

Display Panorama Software Update Information

Select **Panorama > Software** to display the following information. To display the latest information from Palo Alto Networks, click **Check Now**.

Software and Content Update Information	Description
Version	The Panorama software version
Size	The size in megabytes of the software image.
Release Date	The date and time when Palo Alto Networks made the update available.
Available	Indicates whether the image is available for installation.
Currently Installed	A check mark indicates that the update that is installed.
Action	Indicates the actions (Download , Install , or Reinstall) that are available for an image.
Release Notes	Click Release Notes to access the release notes for the desired software release and review the release changes, fixes, known issues, compatibility issues, and changes in default behavior.
<input checked="" type="checkbox"/>	Deletes an update when no longer needed or to free up space for more downloads or uploads.

Panorama > Device Deployment

Select **Panorama > Device Deployment** to display current deployment information for the managed firewalls. They also enable you to manage software and content updates, manage licenses, and schedule content updates on the managed firewalls and Log Collectors.

What do you want to know?	See:
Deploy updates to firewalls and Log Collectors.	Manage Software and Content Updates
See which updates are installed or available for download and installation.	Display Software and Content Update Information
Schedule automatic content updates for firewalls and Log Collectors	Schedule Dynamic Content Updates
View, activate, deactivate, and refresh licenses. See the status of firewall licenses.	Manage Firewall Licenses
Looking for more?	Manage Licenses and Updates 

Manage Software and Content Updates

▲ Panorama > Device Deployment > Software

Select **Panorama > Device Deployment > Software** to deploy software and content updates to managed firewalls and Log Collectors.

Panorama Device Deployment Option	Description
Download	To deploy a software or content update when Panorama is connected to the Internet, Download the update. When the download finishes, the Available column displays Downloaded. You can then: <ul style="list-style-type: none"> • Install the PAN-OS/Panorama software update or content update. • Activate the GlobalProtect Client (GlobalProtect agent/app) or SSL VPN Client software update.
Upgrade	If a BrightCloud URL Filtering content update is available, click Upgrade . After a successful upgrade, you can Install the update on firewalls.
Install	After you download or upload a PAN-OS software, Panorama software, or content update (see Manage Software and Content Updates), click Install in the Action column and select: <ul style="list-style-type: none"> • Devices—Select the firewalls or Log Collectors on which to install the update. If the list is long, use the Filters. Select Group HA Peers to group firewalls that are high availability (HA) peers. This option enables you to easily identify firewalls that have an HA configuration. To display only specific firewalls or Log Collectors, select them and then Filter Selected. • Upload only to device (software only)—Select this option to load the software without automatically installing it. You must manually install the software. • Reboot device after install (software only)—Select this option if you want the installation process to automatically reboot the firewalls or Log Collectors. The installation cannot finish until a reboot occurs. • Disable new apps in content update (Applications and Threats only)—Select this option to disable applications in the update that are new relative to the last installed update. This protects against the latest threats while giving you the flexibility to enable applications after preparing any policy updates. Then, to enable applications, log in to the firewall, select Device > Dynamic Updates, click Apps in the Features column to display the new applications, and click Enable/Disable for each application you want to enable.  You can also select Panorama > Managed Devices to install Firewall Software and Content Updates or Panorama > Managed Collectors to Install a Software Update on a Log Collector .
Activate	After you download or upload a GlobalProtect Client (GlobalProtect agent/app) or SSL VPN Client software update (see Manage Software and Content Updates), click Activate in the Action column and select the options as follows: <ul style="list-style-type: none"> • Devices—Select the firewalls on which to activate the update. If the list is long, use the Filters. Select Group HA Peers to group firewalls that are high availability (HA) peers. This option enables you to easily identify firewalls that have an HA configuration. To display only specific firewalls, select them and then Filter Selected. • Upload only to device—Select this option if you don't want PAN-OS to automatically activate the uploaded image. You must log in to the firewall and activate it.

Panorama Device Deployment Option	Description
Release Notes	Click Release Notes to access the release notes for the desired software release and review the release changes, fixes, known issues, compatibility issues, and changes in default behavior.
Documentation	Click Documentation to access the release notes for the desired content release.
<input checked="" type="checkbox"/>	Deletes software or content updates when no longer needed or when you want to free up space for more downloads or uploads.
Check Now	Check Now to Display Software and Content Update Information .
Upload	To deploy a software or content update when Panorama is not connected to the Internet, download the update to your computer from the Software Updates or Dynamic Updates site, select the Panorama > Device Deployment page that corresponds to the update type, click Upload , select the update Type (content updates only) , select the uploaded file, and click OK . The steps to then install or activate the update depend on the type: <ul style="list-style-type: none"> • PAN-OS or Panorama software—When the upload is complete, the Available column displays Uploaded. You can then install the software update. • GlobalProtect Client or SSL VPN Client software—Activate from file. • Dynamic updates—Install from file.
Install from File	After you upload a content update, click Install from File , select the content Type , select the filename of the update, and select the firewalls or Log Collectors.
Activate from File	After you upload a GlobalProtect Client (GlobalProtect agent/app) or SSL VPN Client software update, click Activate from File , select the filename of the update, and select the firewalls.
Schedules	Select this option to Schedule Dynamic Content Updates .

Display Software and Content Update Information

▲ Panorama > Device Deployment > Software

Select **Panorama > Device Deployment > Software** to display PAN-OS **Software**, **SSL VPN Client** software, **GlobalProtect Client** software, and **Dynamic Updates** (content) currently installed or available for download and installation. The **Dynamic Updates** page organizes the information by content type (Antivirus, Applications and Threats, URL Filtering, and WildFire) and indicates the date and time of the last check for updated information. To display the latest software or content information from Palo Alto Networks, click **Check Now**.

Software and Content Update Information	Description
Version	The software or content update version.
File Name	The name of the update file.
Platform	The designated firewall or Log Collector platform for the update. A number indicates a hardware firewall platform (for example, 7000 indicates the PA-7000 Series firewall), vm indicates the VM-Series firewall, and m indicates the M-Series appliance.
Features	(Content only) Lists the type of signatures the content version might include.
Type	(Content only) Indicates whether the download includes a full database update or an incremental update.
Size	The size of the update file.
Release Date	The date and time when Palo Alto Networks made the update available.
Available	(PAN-OS or Panorama software only) Indicates that the update is downloaded or uploaded.
Downloaded	(SSL VPN Client software, GlobalProtect Client software, or content only) A check mark indicates that the update is downloaded.
Action	Indicates the action you can perform on the update—Download, Upgrade, Install, or Activate.
Documentation	(Content only) Provides a link to the release notes for the desired content release.
Release Notes	(Software only) Provides a link to the release notes for the desired software release.
	Deletes an update when no longer needed or when you want to free up space for more downloads or uploads.

Schedule Dynamic Content Updates

▲ Panorama > Device Deployment > Dynamic Updates

To [schedule an automatic download and installation of an update](#), click **Schedules**, click **Add**, and complete the following fields.

Dynamic Update Schedule Setting	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 this option to disable the scheduled job.
Type	Select the type of content update to schedule— App , App and Threat , Antivirus , WildFire , or URL Database .
Recurrence	Select the interval at which Panorama checks in with the update server. The recurrence options vary by update type.
Time	For a Daily update, select the Time from the 24-hour clock. For a Weekly update, select the Day of week, and the Time from the 24-hour clock.
Disable new apps in content update	You can select this option only if you set the update Type to App or App and Threat and only if Action is set to Download and Install . Select this option to disable applications in the update that are new relative to the last installed update. This protects against the latest threats while giving you the flexibility to enable the applications after preparing any policy updates. Then, to enable applications, log in to the firewall, select Device > Dynamic Updates , click Apps in the Features column to display the new applications, and click Enable/Disable for each application you want to enable.
Action	<ul style="list-style-type: none"> • Download Only—Panorama will download the scheduled update. You must manually “Install” the update on firewalls and Log Collectors. • Download and Install—Panorama will download and automatically install the scheduled update.
Devices	Select Devices and then select the firewalls that will receive scheduled content updates.
Log Collectors	Select Log Collectors and then select the managed collectors that will receive scheduled content updates.

Manage Firewall Licenses

▲ Panorama > Device Deployment > Licenses

Select **Panorama > Device Deployment > Licenses** to perform the following tasks:

- Update licenses of firewalls that don't have direct internet access—Click Refresh.
- Activate a license on firewalls—To activate a license on firewalls, click **Activate**, select the firewalls and, in the Auth Code column, enter the authorization codes that Palo Alto Networks provided for the firewalls.
- Deactivate all the licenses and subscriptions/entitlements installed on VM-Series firewalls—Click **Deactivate VMs**, select the firewalls (the list displays only firewalls running PAN-OS 7.0 or later releases), and click:
 - **Continue**—Deactivates the licenses and automatically registers the changes with the licensing server. The licenses are credited back to your account and are available for reuse.
 - **Complete Manually**—Generates a token file. Use this option if Panorama does not have direct Internet access. To complete the deactivation process, you must log in to the [Support portal](#), select **Assets**, click **Deactivate License(s)**, upload the token file, and click **Submit**. After you complete the deactivation process.

You can also view the current license status for managed firewalls. For firewalls that have direct internet access, Panorama automatically performs a daily check-in with the licensing server, retrieves license updates and renewals, and pushes them to the firewalls. The check-in is hard-coded to occur between 1 and 2 A.M.; you cannot change this schedule.

Firewall License Information	Description
Device	The firewall name.
Virtual System	Indicates whether the firewall does or does not support multiple virtual systems.
Threat Prevention	Indicates whether the license is active , inactive , or expired (along with the expiration date).
URL	
Support	
GlobalProtect Gateway	
GlobalProtect Portal	
WildFire	
VM-Series Capacity	Indicates whether this is or is not a VM-Series firewall.

