



PAN-OS® Web Interface Reference Guide
Release 6.1

Contact Information

Corporate Headquarters:

Palo Alto Networks
4401 Great America Parkway
Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About this Guide

This guide takes you through the configuration and maintenance of your Palo Alto Networks next-generation firewall. 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](http://www.paloaltonetworks.com/documentation).
- For access to the knowledge base, discussion forums, and videos, refer to [https://live.paloaltonetworks.com](http://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](http://www.paloaltonetworks.com/support/tabs/overview.html).
- For the most current PAN-OS 6.1 release notes, go to
[https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os-release-notes.html](http://www.paloaltonetworks.com/documentation/61/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

© 2014–2016 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](http://www.paloaltonetworks.com/company/trademarks.html). All other marks mentioned herein may be trademarks of their respective companies.

Revision Date: September 11, 2017

Table of Contents

Chapter 1

Introduction	11
Firewall Overview.	11
Features and Benefits	12
Management Interfaces	13

Chapter 2

Getting Started	15
Preparing the Firewall	15
Setting Up the Firewall	15
Using the Firewall Web Interface.	17
Committing Changes	19
Navigating to Configuration Pages	20
Using Tables on Configuration Pages	20
Required Fields	20
Locking Transactions	21
Supported Browsers	21
Getting Help Configuring the Firewall	22
Obtaining More Information	22
Technical Support	22

Chapter 3

Device Management.	23
System Setup, Configuration, and License Management	24
Defining Management Settings	24
Defining Operations Settings	37
Defining Hardware Security Modules	41
SNMP	43
Defining Services Settings	44
Defining Content-ID Settings	48
Configuring WildFire Settings	50
Defining Session Settings	51
Session Settings	52
Session Timeouts	53
Decryption Settings: Certificate Revocation Checking	55
Decryption Settings: Forward Proxy Server Certificate Settings.	56

Table of Contents

Comparing Configuration Files	57
Installing a License	58
Defining VM Information Sources	59
Installing the Software	63
Updating Threat and Application Definitions	65
Administrator Roles, Profiles, and Accounts	67
Defining Administrator Roles	68
Defining Password Profiles	69
Username and Password Requirements	71
Creating Administrative Accounts	71
Specifying Access Domains for Administrators	73
Setting Up Authentication Profiles	74
Creating a Local User Database	76
Adding Local User Groups	77
Configuring RADIUS Server Settings	78
Configuring LDAP Server Settings	78
Configuring Kerberos Settings (Native Active Directory Authentication)	79
Setting Up an Authentication Sequence	80
Scheduling Log Exports	81
Defining Logging Destinations	82
Defining Configuration Log Settings	84
Defining System Log Settings	84
Defining HIP Match Log Settings	85
Defining Alarm Log Settings	85
Managing Log Settings	86
Configuring SNMP Trap Destinations	87
Configuring Syslog Servers	89
Custom Syslog Field Descriptions	90
Configuring Email Notification Settings	97
Configuring Netflow Settings	98
Using Certificates	99
Managing Device Certificates	100
Managing the Default Trusted Certificate Authorities	103
Creating a Certificate Profile	103
Adding an OCSP Responder	105
Encrypting Private Keys and Passwords on the Firewall	106
Enabling HA on the Firewall	107
Defining Virtual Systems	117
Configuring Shared Gateways	119
Defining Custom Response Pages	121
Viewing Support Information	122
Chapter 4	
Network Settings	125
Defining Virtual Wires	125
Configuring a Firewall Interface	126
Configuring an Ethernet Interface	126
Configuring an Ethernet Subinterface	134
Configuring a Virtual Wire Interface	140
Configuring a Virtual Wire Subinterface	141
Configuring a Tap Interface	141
Configuring a Log Card Interface	142

Configuring a Decrypt Mirror Interface	143
Configuring Aggregate Interface Groups	143
Configuring an Aggregate Ethernet Interface	146
Configuring an HA Interface	147
Configuring a VLAN Interface	148
Configuring a Loopback Interface	152
Configuring a Tunnel Interface	153
Configuring a Virtual Router	155
Configuring the General tab	155
Configuring the Static Routes tab	156
Configuring the Redistribution Profiles Tab	157
Configuring the RIP Tab	158
Configuring the OSPF Tab	160
Configuring the OSPFv3 Tab	165
Configuring the BGP Tab	170
Configuring the Multicast Tab	178
Defining Security Zones	181
More Runtime Stats for a Virtual Router	183
VLAN Support	189
DHCP Server and Relay	190
DNS Proxy	192
Defining Interface Management Profiles	193
Defining Monitor Profiles	194
Defining Zone Protection Profiles	195
Configuring Flood Protection	196
Configuring Reconnaissance Protection	197
Configuring Packet Based Attack Protection	198
Chapter 5	
Policies and Security Profiles	203
Policy Types	203
Guidelines on Defining Policies	204
Specifying Users and Applications for Policies	206
Defining Policies on Panorama	207
Defining Security Policies	208
General Tab	208
Source Tab	209
User Tab	210
Destination Tab	211
Application Tab	211
Service/URL Category Tab	212
Actions Tab	213
NAT Policies	215
Determining Zone Configuration in NAT and Security Policy	217
NAT Rule Options	217
NAT Policy Examples	218
NAT64	218
Defining Network Address Translation Policies	219
General Tab	219
Original Packet Tab	220
Translated Packet Tab	220
Policy-Based Forwarding Policies	222

Table of Contents

General Tab	222
Source Tab.....	223
Destination/Application/Service Tab	224
Forwarding Tab.....	224
Decryption Policies	225
General Tab	226
Source Tab.....	226
Destination Tab	227
URL Category Tab.....	228
Options Tab.....	228
Defining Application Override Policies	228
General Tab	229
Source Tab.....	229
Destination Tab	230
Protocol/Application Tab	230
Defining Captive Portal Policies	230
General Tab	231
Source Tab.....	232
Destination Tab	232
Service/URL Category Tab.....	232
Action Tab	233
Defining DoS Policies	233
General Tab	233
Source Tab.....	235
Destination Tab	236
Options/Protection Tab.....	236
Security Profiles	237
Antivirus Profiles	238
Antivirus Profile Page	239
Antivirus Tab	239
Exceptions Tab.....	240
Anti-spyware Profiles	240
Vulnerability Protection Profiles	243
URL Filtering Profiles	246
File Blocking Profiles	251
Data Filtering Profiles	256
DoS Profiles	258
Other Policy Objects.....	260
Defining Address Objects	261
Defining Address Groups	262
Defining Regions	264
Applications and Application Groups	266
Defining Applications.....	270
Defining Application Groups.....	273
Application Filters	273
Services	274
Service Groups	276
Working with Tags	276
Data Patterns	277
Dynamic Block Lists.....	279
Custom Spyware and Vulnerability Signatures	281
Defining Data Patterns	282
Defining Spyware and Vulnerability Signatures.....	282

Custom URL Categories	285
Security Profile Groups	287
Log Forwarding	288
Decryption Profiles	290
Schedules	292
Chapter 6	
Reports and Logs	295
Using the Dashboard	296
Using the Application Command Center.....	297
Using App Scope	301
Summary Report.....	302
Change Monitor Report	303
Threat Monitor Report	304
Threat Map Report.....	306
Network Monitor Report.....	307
Traffic Map Report	309
Viewing the Logs.....	310
Viewing Session Information.....	314
Working with Botnet Reports	314
Managing Botnet Reports.....	314
Configuring the Botnet Report	315
Managing PDF Summary Reports.....	317
Managing User/Group Activity Reports.....	319
Managing Report Groups.....	320
Scheduling Reports for Email Delivery	321
Viewing Reports	321
Generating Custom Reports	322
Taking Packet Captures	323
Chapter 7	
Configuring the Firewall for User Identification.....	327
Configuring the Firewall for User Identification	327
User Mapping Tab.....	328
User-ID Agents Tab	334
Terminal Services Agents Tab	336
Group Mapping Tab	337
Captive Portal Settings Tab.....	338
Chapter 8	
Configuring IPSec Tunnels.....	343
Defining IKE Gateways	343
IKE Gateway General Tab	344
IKE Gateway Advanced Phase 1 Options Tab	344
Setting Up IPSec Tunnels	345

Table of Contents

IPSec Tunnel General Tab	345
IPSec Tunnel Proxy ID Tab	347
Viewing IPSec Tunnel Status on the Firewall	348
Defining IKE Crypto Profiles	348
Defining IPSec Crypto Profiles	349
Chapter 9	
GlobalProtect Settings.....	351
Setting Up the GlobalProtect Portal	351
Portal Configuration Tab.....	351
Client Configuration Tab	353
Satellite Configuration Tab.....	359
Setting Up the GlobalProtect Gateways	361
General Tab	361
Client Configuration Tab	362
Satellite Configuration Tab.....	365
Setting Up Gateway Access to a Mobile Security Manager	367
Creating HIP Objects	369
General Tab	369
Mobile Device Tab	370
Patch Management Tab	372
Firewall Tab.....	372
Antivirus Tab	373
Anti-Spyware Tab.....	374
Disk Backup Tab	374
Disk Encryption Tab.....	375
Data Loss Prevention Tab	375
Custom Checks Tab	376
Setting Up HIP Profiles	377
Setting Up and Activating the GlobalProtect Agent	378
Setting Up the GlobalProtect Agent	380
Using the GlobalProtect Agent	380
Chapter 10	
Configuring Quality of Service	381
Configuring QoS for Firewall Interfaces	381
Defining QoS Profiles	383
Defining QoS Policies	384
Displaying QoS Statistics	387
Chapter 11	
Central Device Management Using Panorama.....	389
Panorama Tab	391
Switching Device Context	393
Setting Up Storage Partitions	394
Configuring High Availability (HA)	394
Adding Devices	396

Backing Up Firewall Configurations	398
Defining Device Groups	399
Shared Objects and Policies	400
Applying Policy to a Specific Device in a Device Group.....	401
Defining Panorama Administrator Roles	402
Creating Panorama Administrative Accounts	403
Specifying Panorama Access Domains for Administrators	405
Committing your Changes in Panorama	405
Templates	407
Overriding Template Settings	408
Deleting Templates.....	409
Logging and Reporting.....	409
Enable Log Forwarding.....	410
Managing Log Collectors	413
Adding a Log Collector	413
Installing a Software Update on a Collector	418
Defining Log Collector Groups	418
Generating User Activity Reports.....	420
Viewing Firewall Deployment Information	421
Scheduling Dynamic Updates	422
Scheduling Configuration Exports.....	422
Upgrading the Panorama Software.....	424
Register VM-Series Firewall as a Service on the NSX Manager	425
Updating Information from the VMware Service Manager.....	427
 Appendix A	
Custom Pages	429
Antivirus and Anti-spyware Block Page	429
Application Block Page	431
File Blocking Block Page	431
SSL Decryption Opt-out Page	432
Captive Portal Comfort Page	432
SSL VPN Login Page	432
SSL Certificate Revoked Notify Page	434
URL Filtering and Category Match Block Page	434
URL Filtering Continue and Override Page	435
URL Filtering Safe Search Enforcement Block Page	436
 Appendix B	
Application Categories, Subcategories, Technologies, and Characteristics	437
Application Categories and Subcategories	437
Application Technologies	439
Application Characteristics	439
 Appendix C	
Common Criteria/Federal Information Processing Standards Support .	441

Table of Contents

Enabling CC/FIPS Mode	441
CC/FIPS Security Functions	442
Appendix D	
Open Source Licenses	443
Artistic License.....	444
BSD	445
GNU General Public License.....	446
GNU Lesser General Public License	450
MIT/X11	456
OpenSSH.....	456
PSF	460
PHP	460
Zlib	461
Appendix E	
Firewall Access to External Web Resources.....	463
Application Database.....	464
Threat/Antivirus Database	464
PAN-DB URL Filtering Database.....	464
BrightCloud URL Filtering Database.....	464
WildFire	464
Index	467

Chapter 1

Introduction

This section provides an overview of the firewall:

- [“Firewall Overview”](#)
- [“Features and Benefits”](#)
- [“Management Interfaces”](#)

Firewall Overview

The Palo Alto Networks firewall allows you to specify security policies based on accurate identification of each application seeking access to your network. Unlike traditional firewalls that identify applications only by protocol and port number, the 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 non-standard ports.

For example, you can define security policies for specific applications, rather than rely on 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 firewall provides granular control over the traffic allowed to access your network. The primary features and benefits include:

- **Application-based policy enforcement**—Access control by application is far more effective when application identification is based on more than just protocol and port number. High risk applications can be blocked, as well as high risk behavior, such as file-sharing. Traffic encrypted with the s Layer (SSL) protocol can be decrypted and inspected.
- **User Identification (User-ID)**—User-ID 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. This information can then be used to provide an invaluable method of providing 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 no other organizations in the company would be able to use that application. You can also configure granular control of certain components of an application based on users and groups. See “[Configuring the Firewall for User Identification](#)”.
- **Threat prevention**—Threat prevention services that protect the network from viruses, worms, spyware, and other malicious traffic can be varied by application and traffic source (see “[Security Profiles](#)”).
- **URL filtering**—Outbound connections can be filtered to prevent access to inappropriate web sites (see “[URL Filtering Profiles](#)”).
- **Traffic visibility**—Extensive reports, logs, and notification mechanisms provide detailed visibility into network application traffic and security events. The Application Command Center (ACC) in the web interface identifies the applications with the most traffic and the highest security risk (see “[Reports and Logs](#)”).
- **Networking versatility and speed**—The 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. Multi-gigabit speeds and a single-pass architecture provide all services with little or no impact on network latency.
- **GlobalProtect**—GlobalProtect 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 support provides automatic failover in the event of any hardware or software disruption (see “[Enabling HA on the Firewall](#)”).
- **Malware analysis and reporting**—WildFire provides detailed analysis and reporting on malware that traverses the firewall.
- **VM-Series Firewall**—Provides a virtual instance of PAN-OS positioned for use in a virtualized data center environment and particularly well suited for private and public cloud deployments. Installs on any x86 device that is capable of running VMware ESXi, without the need to deploy Palo Alto Networks hardware.

- **Management and Panorama**—Each firewall is managed through an intuitive web interface or a command-line interface (CLI), or all devices can be centrally managed through the Panorama centralized management system, which has a web interface very similar to the device web interface.

Management Interfaces

The firewall supports the following management interfaces. See “[Supported Browsers](#)” for a list of supported browsers.

- **Web interface**—Configuration and monitoring over HTTP or HTTPS from a web browser.
- **CLI**—Text-based configuration and monitoring over Telnet, Secure Shell (SSH), or the console port (see the [PAN-OS Command Line Interface Reference Guide](#)).
- **Panorama**—Palo Alto Networks product that provides web-based management, reporting, and logging for multiple firewalls. The Panorama interface is similar to the device web interface, with additional management functions included. See “[Central Device Management Using Panorama](#)” for information on using Panorama.
- **Simple Network Management Protocol (SNMP)**—Palo Alto Networks products support SNMPv2c and SNMPv3, read-only access over SNMP, and support for SNMP traps. See “[Configuring SNMP Trap Destinations](#)”.
- **Syslog**—Provides message generation for one or more remote syslog servers (see “[Configuring Syslog Servers](#)”).
- **XML API**—Provides a Representational State Transfer (REST)-based interface to access device configuration, operational status, reports, and packet captures from the firewall. There is an API browser available on the firewall at <https://<firewall>/api>, where <firewall> is the host name or IP address of the firewall. This link provides help on the parameters required for each type of API call. See the [XML API Usage Guide](#) for more information.

Chapter 2

Getting Started

This chapter describes how to set up and start using the firewall:

- “[Preparing the Firewall](#)”
- “[Setting Up the Firewall](#)”
- “[Using the Firewall Web Interface](#)”
- “[Getting Help Configuring the Firewall](#)”

Preparing the Firewall

Perform the following tasks to prepare the firewall for setup:

1. Mount the firewall in a rack and power it up as described in the *Hardware Reference Guide* for your [platform](#).
2. Register your firewall at <https://support.paloaltonetworks.com> to obtain the latest software and App-ID updates, and to activate support or subscriptions with the authorization codes emailed to you.
3. Obtain an IP address from your network administrator for configuring the management port on the firewall.

Setting Up the Firewall

To perform the initial firewall setup:

1. Connect your computer to the management port (MGT) on the firewall using an RJ-45 Ethernet cable.
2. Start your computer. Assign a static IP address to your computer on the 192.168.1.0 network (for example, 192.168.1.5) with a netmask of 255.255.255.0.
3. Launch a supported web browser and enter <https://192.168.1.1>.

The browser automatically opens the Palo Alto Networks login page.

4. Enter **admin** in both the **Name** and **Password** fields, and click **Login**. The system presents a warning that the default password should be changed. Click **OK** to continue.
5. On the **Device** tab, choose **Setup** and configure the following (for general instructions on configuring settings in the web interface, see “[Using the Firewall Web Interface](#)”):
 - On the **Management** tab under **Management Interface Settings**, enter the firewall’s IP address, netmask, and default gateway.
 - On the **Services** tab, enter the IP address of the Domain Name System (DNS) server. Enter the IP address or host and domain name of the Network Time Protocol (NTP) server and select your time zone.
 - Click **Support** on the side menu.
If this is the first Palo Alto Networks firewall for your company, click **Register Device** to register the firewall. (If you have already registered a firewall, you have received a user name and password.)
Click the **Activate support using authorization codes** link and enter the authorization codes that have been emailed to you for any optional features. Use a space to separate multiple authorization codes.
6. Click **Administrators** under the **Devices** tab.
7. Click **admin**.
8. In the **New Password** and **Confirm New Password** fields, enter and confirm a case-sensitive password (up to 15 characters).
9. Click **OK** to submit the new password.
10. Commit the configuration to make these settings active. When the changes are committed, the firewall will be reachable through the IP address assigned in Step 5. For information on committing changes, see “[Committing Changes](#)”.



The default configuration of the firewall when delivered from the factory, or after a factory reset is performed, is a virtual wire between Ethernet ports 1 and 2 with a default policy to deny all inbound traffic and allow all outbound traffic.

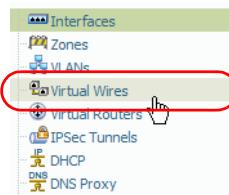
Using the Firewall Web Interface

The following conventions apply when using the firewall interface.

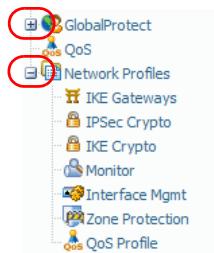
- To display the menu items for a general functional category, click the tab, such as **Objects** or **Device**, near the top of the browser window.



- Click an item on the side menu to display a panel.



- To display submenu items, click the icon to the left of an item. To hide submenu items, click the icon to the left of the item.



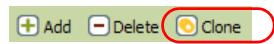
- On most configuration pages, you can click **Add** to create a new item.



- To delete one or more items, select their check boxes and click **Delete**. In most cases, the system prompts you to confirm by clicking **OK** or to cancel the deletion by clicking **Cancel**.



- On some configuration pages, you can select the check box for an item and click **Clone** to create a new item with the same information as the selected item.



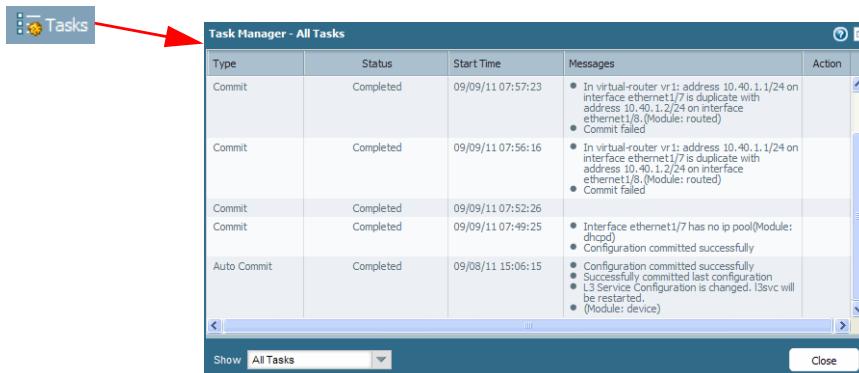
- To modify an item, click its underlined link.

Name	Location	Protocol
service-http	Predefined	TCP
<u>service-https</u>	Predefined	TCP

- To view help information on a page, click the **Help** icon in upper right area of the page.



- To view the current list of tasks, click the **Tasks** icon in the lower right corner of the page. The Task Manager window opens to show the list of tasks, along with status, start times, associated messages, and actions. Use the **Show** drop-down list to filter the list of tasks.



- The web interface language is controlled by the current language of the computer that is managing the device if a specific language preference has not been defined. For example, if the computer you use to manage the firewall has a locale of Spanish, when you log in to the firewall, the web interface will be in Spanish.

To specify a language that will always be used for a given account regardless of the locale of the computer, click the **Language** icon in the lower right corner of the page and the Language Preference window opens. Click the drop-down list to select the desired language and then click **OK** to save your change.



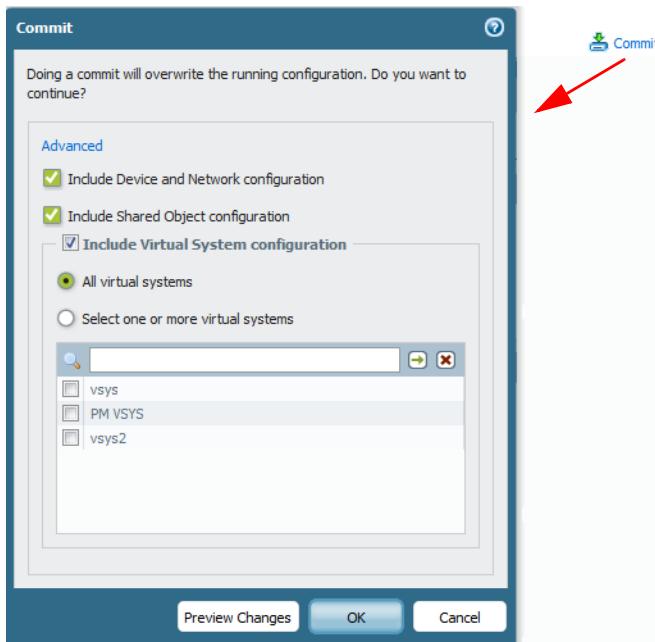
- On pages that list information you can modify (for example, the **Setup** page on the **Devices** tab), click the icon in the upper right corner of a section to edit the settings.



- After you configure settings, you must click **OK** or **Save** to store the changes. When you click **OK**, the current “candidate” configuration is updated.

Committing Changes

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



Optionally, you can **Preview Changes** to bring up a two-pane window that shows proposed changes in the candidate configuration compared to the current running configuration. You can choose the number of lines of context to display or show all lines. The window displays the configurations side by side in separate panes and uses colors to highlight the differences line by line. The **Device > Config Audit** feature performs the same function (see “[Comparing Configuration Files](#)”).



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

Click the **Advanced** link if you want to display the following commit options:

- Include Device and Network configuration**—Include the device and network configuration changes in the commit operation.
- Include Shared Object configuration**—(Multi-virtual system firewalls only) Include the shared object configuration changes in the commit operation.

- **Include Policy and Objects**—(Non-multi-virtual system firewalls only) Include the policy and object configuration changes in the commit operation.



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

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

For more information about committing changes, see “[Defining Operations Settings](#)”.

Navigating to Configuration Pages

Each configuration section in this guide shows the menu path to the configuration page. For example, to reach the **Vulnerability Protection** page, choose the **Objects** tab and then choose **Vulnerability Protection** under **Security Profiles** in the side menu. This is indicated in this guide by the following path:

- *Objects > Security Profiles > Vulnerability Protection*

Using Tables on Configuration Pages

The tables on configuration pages include sorting and column chooser options. Click a column header to sort on that column, and click again to change the sort order. Click the arrow to the right of any column and select check boxes to choose the columns to display.

Direction	Default Action	Comment
Sort Ascending		
Sort Descending		

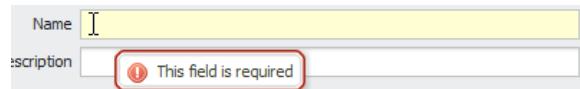
Columns

Adjust Columns

Location
 Severity
 Direction
 Default Action
 Comment

Required Fields

Required fields are shown with a light yellow background. A message indicating that the field is required appears when you hover over or click in the field entry area.



Locking Transactions

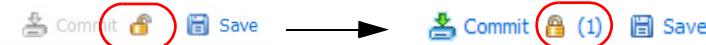
The web interface provides support for multiple administrators by allowing an administrator to lock a current set of transactions, thereby preventing configuration changes or commit operations by another administrator until the lock is removed. The following types of locks are supported:

- **Config lock**—Blocks other administrators from making changes to the configuration. This type of lock can be set globally or for a virtual system. It can be removed only by the administrator who set it or by a superuser on the system.
- **Commit Lock**—Blocks other administrators from committing changes until all of the locks have been released. This type of lock prevents collisions that can occur when two administrators are making changes at the same time and the first administrator finishes and commits changes before the second administrator has finished. The lock is released when the current changes are committed by the administrator who applied the lock, or it can be released manually.

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

To lock a transaction, click the unlocked icon on the top bar to open the Locks dialog box. Click **Take a Lock**, select the scope of the lock from the drop-down list, and click **OK**. Add additional locks as needed, and then click **Close** to close the Lock dialog box.

The transaction is locked, and the icon on the top bar changes to a locked icon that shows the number of locked items in parentheses.



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

You can arrange to automatically acquire a commit lock by selecting the **Automatically acquire commit lock** check box in the Management area of the **Device Setup** page. See “[System Setup, Configuration, and License Management](#)”.

Supported Browsers

The following web browsers are supported for access to the firewall web interface:

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

Getting Help Configuring the Firewall

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

Obtaining More Information

To obtain more information about the firewall, see the following:

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

Technical Support

For technical support, for information on support programs, or to manage your account or devices, go to <https://support.paloaltonetworks.com>.

Chapter 3

Device Management

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

- “System Setup, Configuration, and License Management”
- “Defining VM Information Sources”
- “Installing the Software”
- “Updating Threat and Application Definitions”
- “Administrator Roles, Profiles, and Accounts”
- “Setting Up Authentication Profiles”
- “Setting Up an Authentication Sequence”
- “Creating a Certificate Profile”
- “Scheduling Log Exports”
- “Defining Logging Destinations”
- “Defining Alarm Log Settings”
- “Configuring Netflow Settings”
- “Using Certificates”
- “Encrypting Private Keys and Passwords on the Firewall”
- “Enabling HA on the Firewall”
- “Defining Virtual Systems”
- “Defining Custom Response Pages”
- “Viewing Support Information”

System Setup, Configuration, and License Management

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

- “[Defining Management Settings](#)”
- “[Defining Operations Settings](#)”
- “[Defining Hardware Security Modules](#)”
- “[SNMP](#)”
- “[Defining Services Settings](#)”
- “[Defining Content-ID Settings](#)”
- “[Configuring WildFire Settings](#)”
- “[Defining Session Settings](#)”
- “[Comparing Configuration Files](#)”
- “[Installing a License](#)”

Defining Management Settings

- ▶ *Device > Setup > Management*
- ▶ *Panorama > Setup > Management*

On a firewall, use the **Device > Setup > Management** tab to configure management settings.

On Panorama, use the **Device > Setup > Management** tab to configure managed firewalls via Panorama templates. Use the **Panorama > Setup > Management** tab to configure settings for Panorama itself.



For firewall management, optionally you can use the IP address of a loopback interface instead of the management port (see “[Configuring a Loopback Interface](#)”).

Table 1. Management Settings

Item	Description
General Settings	
Hostname	Enter a host name (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Domain	Enter the Fully Qualified Domain Name (FQDN) of the firewall (up to 31 characters).
Login Banner	Enter custom text that will be displayed on the firewall login page. The text is displayed below the Name and Password fields.
Time Zone	Select the time zone of the firewall.

Table 1. Management Settings (Continued)

Item	Description
Locale	Select a language for PDF reports from the drop-down list. See "Managing PDF Summary Reports" . If you have a specific language preference set for the web interface, PDF reports will still use the language specified in this locale setting. See language preference in "Using the Firewall Web Interface" .
Time	To set the date and time on the firewall, click Set Time . Enter the current date in (YYYY/MM/DD) or click the calendar icon  to select a month and day. Enter the current time in 24-hour format (HH:MM:SS). You can also define an NTP server from Device > Setup > Services .
Serial Number (virtual machines only)	Enter the serial number of the firewall/Panorama. Find the serial number in the order fulfillment email that was sent to you.
Geo Location	Enter the latitude (-90.0 to 90.0) and longitude (-180.0 to 180.0) of the firewall.
Automatically acquire commit lock	Automatically apply a commit lock when you change the candidate configuration. For more information, see "Locking Transactions" .
Certificate Expiration Check	Instruct the firewall to create warning messages when on-box certificates near their expiration dates.
Multi Virtual System Capability	Enables the use of multiple virtual systems (if the firewall model supports that feature). For details, see "Defining Virtual Systems" .
URL Filtering Database (Panorama only)	Select a URL filtering vendor to enable on Panorama: brightcloud or paloaltonetworks (PAN-DB).
Authentication Settings	
Authentication Profile	Select the authentication profile to use for administrator access to the firewall. For instructions on configuring authentication profiles, see "Setting Up Authentication Profiles" .
Certificate Profile	Select the certificate profile to use for administrator access to the firewall. For instructions on configuring certificate profiles, see "Creating a Certificate Profile" .
Idle Timeout	Enter the 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. WARNING! 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.
Failed Attempts	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. CAUTION: If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, the Failed Attempts is ignored and the user is never locked out.

Table 1. Management Settings (Continued)

Item	Description
Lockout Time	<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>CAUTION: If you set the Lockout Time to a value other than 0 but leave the Failed Attempts at 0, the Lockout Time is ignored and the user is never locked out.</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 timeouts and object sharing settings on Panorama: see “ Panorama Settings: Panorama > Setup > Management ”.	
<p>Note: The firewall uses an SSL connection with AES-256 encryption to register with Panorama. Panorama and the firewall authenticate each other using 2,048-bit certificates and use the SSL connection for configuration management and log collection.</p>	
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 for receiving TCP messages from Panorama (1-240 seconds, default 240).
Send Timeout for Connection to Panorama	Enter the timeout for sending TCP messages to Panorama (1-240 seconds, default 240).
Retry Count for SSL Send to Panorama	Enter the number of retries for attempts to send Secure Socket Layer (SSL) messages to Panorama (1-64, default 25).
Disable/Enable Panorama Policy and Objects	<p>This button appears when you edit the Panorama Settings on a firewall (not in a template on Panorama). By default, Panorama propagates the policies and objects that are defined for a device group to the firewalls assigned to that group. Clicking Disable Panorama Policy and Objects disables that propagation. By default, this operation also removes those policies and objects from the firewall.</p> <p>To keep a local copy of the device group policies and objects on the firewall before disabling propagation, in the dialog box that the button opens, select the Import Panorama Policy and Objects before disabling check box. Then, when you click OK, PAN-OS copies the policies and objects to the current candidate configuration. After you perform a commit, the policies and objects become part of the firewall configuration: Panorama no longer manages them.</p> <p>Under normal operating conditions, disabling Panorama management is unnecessary and could complicate the maintenance and configuration of the firewall. This option generally applies to situations where the firewall requires rules and object values that differ from those defined in the device group. An example situation 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>

Table 1. Management Settings (Continued)

Item	Description
Disable/Enable Device and Network Template	This button appears when you edit the Panorama Settings on a firewall (not in a template on Panorama). By default, Panorama propagates the device and network configurations defined for a template to the firewalls assigned to that template. Clicking Disable Device and Network Template disables that propagation. By default, this operation also removes the template information from the firewall.
	To keep a local copy of the template information on the firewall before disabling propagation, in the dialog box that the button opens, select the Import Device and Network Templates before disabling check box. Then, when you click OK , PAN-OS copies the information defined in the template to the current candidate configuration on the firewall. After you perform a commit, the template information becomes part of the firewall configuration: Panorama no longer manages that information.
	Under normal operating conditions, disabling Panorama management is unnecessary and could complicate the maintenance and configuration of the firewall. This option generally applies to situations where the firewall requires rules and object values that differ from those defined in the device group. An example situation is when you move a firewall out of production and into a laboratory environment for testing.
	To make the firewall resume accepting templates, click Enable Device and Network Templates .

Panorama Settings: Panorama > Setup > Management

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

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

Receive Timeout for Connection to Device	Enter the timeout for receiving TCP messages from all managed firewalls (1-240 seconds, default 240).
Send Timeout for Connection to Device	Enter the timeout for sending TCP messages to all managed firewalls (1-240 seconds, default 240).
Retry Count for SSL Send to Device	Enter the number of retries for attempts to send Secure Socket Layer (SSL) messages to managed firewalls (1-64, default 25).
Share Unused Address and Service Objects with Devices	Select this check box to share all Panorama shared objects and device group-specific objects with managed firewalls. This setting is enabled by default. If you clear the check box, PAN-OS checks Panorama policies for references to address, address group, service, and service group objects, and does not share any unreferenced objects. This option reduces the total object count by ensuring that PAN-OS sends only necessary objects to managed firewalls.
Shared Objects Take Precedence	Select the check box to specify that shared objects take precedence over device group objects. In this case, device group objects cannot override corresponding objects of the same name from a shared location; PAN-OS discards any device group object with the same name as a shared object. By default, this system-wide setting is disabled: device groups override corresponding shared objects of the same name.

Table 1. Management Settings (Continued)

Item	Description
Management Interface Settings	
This interface applies to the firewall, Panorama M-100 appliance, or Panorama virtual appliance.	
By default, the M-100 appliance uses the management (MGT) interface for configuration, log collection, and collector group communication. However, if you configure Eth1 or Eth2 for log collection and/or collector group communication, it is a best practice to define a separate subnet for the MGT interface that is more private than the Eth1 or Eth2 subnets. You define the subnet in the Netmask (for IPv4) or IPv6 Address/Prefix Length (for IPv6) field. The Panorama virtual appliance does not support separate interfaces.	
<i>Note:</i> To complete the configuration of the management interface, you must specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway. If you commit a partial configuration (for example, you might omit the default gateway), you can only access the device via the console port for future configuration changes. It is recommended that you commit a complete configuration.	
IP Address (IPv4)	If your network uses IPv4, assign an IPv4 address to the management port. Alternatively, you can assign the IP address of a loopback interface for device management. By default, this is the source address for log forwarding.
Netmask (IPv4)	If you assigned an IPv4 address to the management port, enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to the management port, assign an IPv4 address to the default router (it must be on the same subnet as the management port).
IPv6 Address/Prefix Length	If your network uses IPv6, assign an IPv6 address to the management port. 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 port, assign an IPv6 address to the default router (it must be on the same subnet as the management port).
Speed	Configure a data rate and duplex option for the management interface. The choices include 10Mbps, 100Mbps, and 1Gbps at full or half duplex. Use the default auto-negotiate setting to have the device (Panorama or the firewall) determine the interface speed. 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 576-1500, default 1500).
Services	Select the services you want enabled on the specified management interface address: HTTP, HTTP OCSP, HTTPS, Telnet, SSH (Secure Shell), Ping, SNMP, User-ID, User-ID Syslog Listener-SSL, User-ID Syslog Listener-UDP.
Permitted IP Addresses	Enter the list of IP addresses from which firewall management is allowed. When using this option for the Panorama M-100 appliance, add the IP address of each managed firewall, otherwise the firewall cannot connect and forward logs to Panorama or receive configuration updates.

Table 1. Management Settings (Continued)

Item	Description
Eth1 Interface Settings	
This interface only applies to the Panorama M-100 appliance, not the Panorama virtual appliance or the firewall. By default, the M-100 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 and/or collector group communication when you define managed collectors (Panorama > Managed Collectors).	
<i>Note:</i> You cannot commit the Eth1 configuration unless you specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway.	
Eth1	Select this check box to enable the Eth1 interface.
IP Address (IPv4)	If your network uses IPv4, assign an IPv4 address to the Eth1 port.
Netmask (IPv4)	If you assigned an IPv4 address to the port, enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to the port, assign an IPv4 address to the default router (it must be on the same subnet as the Eth1 port).
IPv6 Address/Prefix Length	If your network uses IPv6, assign an IPv6 address of the Eth1 port. 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 port, assign an IPv6 address to the default router (it must be on the same subnet as the Eth1 port).
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 576-1500, default 1500).
Services	Select Ping if you want to enable that service on the Eth1 interface.
Permitted IP Addresses	Enter the list of IP addresses from which Eth1 management is allowed.
Eth2 Interface Settings	
This interface only applies to the Panorama M-100 appliance, not the Panorama virtual appliance or the firewall. By default, the M-100 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).	
<i>Note:</i> You cannot commit the Eth2 configuration unless you specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway.	
Eth2	Select this check box to enable the Eth2 interface.
IP Address (IPv4)	If your network uses IPv4, assign an IPv4 address to the Eth2 port.
Netmask (IPv4)	If you assigned an IPv4 address to the port, enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to the port, assign an IPv4 address to the default router (it must be on the same subnet as the Eth2 port).

Table 1. Management Settings (Continued)

Item	Description
IPv6 Address/Prefix Length	If your network uses IPv6, assign an IPv6 address to the Eth2 port. 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 port, assign an IPv6 address to the default router (it must be on the same subnet as the Eth2 port).
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 576-1500, default 1500).
Services	Select Ping if you want to enable that service on the Eth2 interface.
Permitted IP Addresses	Enter the list of IP addresses from which Eth2 management is allowed.

Table 1. Management Settings (Continued)

Item	Description
Logging and Reporting Settings Use this section of the interface to modify the following options: <ul style="list-style-type: none">• Log storage quotas for a firewall (Device > Setup > Management).• Log storage quotas for a Panorama virtual appliance or an M-100 appliance in Panorama mode (Panorama > Setup > Management). <p><i>Note:</i> To configure the quotas for each log type on an M-100 appliance in log collector mode, select Panorama > Collector Groups > General and select the Log Storage link. See “Installing a Software Update on a Collector”.</p> <ul style="list-style-type: none">• Attributes for calculating and exporting user activity reports.• Predefined reports created on the firewall/Panorama.	

Table 1. Management Settings (Continued)

Item	Description
Log Storage subtab (The PA-7050 firewall has Log Card Storage and Management Card Storage tabs)	<p>Specify the percentage of space allocated to each log type on the hard disk.</p> <p>When you change a percent 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 attempt to save the settings. If this occurs, readjust the percentages so the total is within the 100% limit.</p> <p>Click OK to save settings and Restore Defaults to restore all of the default settings.</p> <p>The PA-7050 firewall stores logs in the Log Processing Card (LPC) and Switch Management Card (SMC), and so divides log quotas into these two areas. The Log Storage tab has quota settings for data type traffic stored on the LPC (for example, traffic and threat logs). The Management Card Storage has quota settings for management type traffic stored on the SMC (for example, the config logs, system logs, and alarms logs).</p> <p><i>Note: When a log reaches the maximum size, the firewall starts overwriting the oldest log entries with the new log entries. If you reduce a log size, the firewall removes the oldest logs when you commit the changes.</i></p>

Table 1. Management Settings (Continued)

Item	Description
Log Export and Reporting subtab	<p>Number of Versions for Config Audit—Enter the number of configuration versions to save before discarding the oldest ones (default 100). You can use these saved versions to audit and compare changes in configuration.</p> <p>Max Rows in CSV Export—Enter the maximum number of rows that will appear in the CSV reports generated from the Export to CSV icon in the traffic logs view (range 1-1048576, default 65535).</p> <p>Max Rows in User Activity Report—Enter the maximum number of rows that is supported for the detailed user activity reports (1-1048576, default 5000).</p> <p>Number of Versions for Config Backups—(Panorama only) Enter the number of configuration backups to save before discarding the oldest ones (default 100).</p> <p>Average Browse Time (sec)—Configure this variable to adjust how browse time is calculated in the “User Activity Report”.</p> <p>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”.</p> <p>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.</p> <p>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.</p> <p>(Range 0-300 seconds, default 60 seconds)</p> <p>Page Load Threshold (sec)—This option allows you to adjust the assumed time it takes for page elements to load on the page. Any request that occurs between the first page load and the page load threshold is assumed to be elements of the page. Any requests that occur outside of the page load threshold is assumed to be the user clicking a link within the page. The page load threshold is also used in the calculations for the “User Activity Report”.</p> <p>(Range 0-60 seconds, default 20 seconds)</p> <p>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.</p> <p>Stop Traffic when LogDb full—Select the check box if you want traffic through the firewall to stop when the log database is full (default off).</p>

Table 1. Management Settings (Continued)

Item	Description
	<p>Enable Log on High DP Load—Select this check box if you would like a system log entry generated when the packet processing load on the firewall is at 100% CPU utilization.</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>
(Only on Panorama)	<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-100 appliance in Panorama mode.</p>
	<p>Pre-Defined Reports—Pre-defined reports for application, traffic, threat, and URL Filtering are available on the firewall and on Panorama. By default, these pre-defined reports are enabled.</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 the check box for the report.</p> <p>Use the Select All or Deselect All options to entirely enable or disable the generation of pre-defined reports.</p> <p><i>Note:</i> Before disabling a report make sure that the report is not included in a Group Report or a PDF Report. If a pre-defined report is part of a set of reports and it is disabled, the entire set of reports will have no data.</p>

Table 1. Management Settings (Continued)

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 “Defining Password Profiles” and see “Username and Password Requirements” for information on valid characters that can be used for accounts.</p> <p><i>Note: The maximum password length that can be entered is 31 characters. When setting requirements, make sure you do not create a combination that will not be accepted. Example, you would not be able to set a requirement of 10 uppercase, 10 lower case, 10 numbers, and 10 special characters since that would exceed the maximum length of 31.</i></p> <p><i>Note: If you have High Availability (HA) configured, always use the primary device when configuring password complexity options and commit soon after making changes.</i></p> <p><i>Note: Minimum password complexity settings do not apply to local database accounts for which you specified a Password Hash (see “Creating a Local User Database”).</i></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. The 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 check box to prevent the account username (or reversed version of the name) from being used in the password.
New Password Differs By Characters	When administrators change their passwords, the characters must differ by the specified value.
Require Password Change on First Login	Select this check box to prompt the administrators to change their passwords the first time they log in to the device.

Table 1. Management Settings (Continued)

Item	Description
Prevent Password Reuse Limit	Require that a previous password is not reused based on the specified count. Example, if the value is set to 4, you could not reuse the any of your last 4 passwords (range 0-50).
Block Password Change Period (days)	User cannot change their passwords until the specified number of days has been reached (range 0-365 days).
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 0-30 days).
Allowed expired admin login (count)	Allow the administrator to log in the specified number of times after the account has expired. Example, if the value is set to 3 and their account has expired, they can log in 3 more times before their account is locked out (range 0-3 logins).
Post Expiration Grace Period (days)	Allow the administrator to log in the specified number of days after the account has expired (range 0-30 days).

Defining Operations Settings

- *Device > Setup > Operations*
- *Panorama > Setup > Operations*

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

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

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



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

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

Table 2. Configuration Management Functions

Function	Description
Configuration Management	
Validate candidate config	Checks the candidate configuration for errors.
Revert to last saved config	Restores the last saved candidate configuration from the local drive. The current candidate configuration is overwritten. An error occurs if the candidate configuration has not been saved.
Revert to running config	Restores the last running configuration. The current running configuration is overridden.
Save named configuration snapshot	Saves the candidate configuration to a file. Enter a file name or select an existing file to be overwritten. Note that the current active configuration file (<i>running-config.xml</i>) cannot be overwritten.

Table 2. Configuration Management Functions (Continued)

Function	Description
Save candidate config	Saves the candidate configuration in flash memory (same as clicking Save at the top of the page).
Load named configuration snapshot (firewall) 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 Encrypting Private Keys and Passwords on the Firewall). 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) 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 Encrypting Private Keys and Passwords on the Firewall). 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 active configuration (<i>running-config.xml</i>) or a previously saved or imported configuration. Select the configuration file to be exported. You can open the file and/or save it in any network location.
Export configuration version	Exports a specified version of the configuration.
Export Panorama and devices config bundle (Panorama only)	Manually generates and exports the latest versions of the running configuration backup of Panorama and of each managed firewall. To automate the process of creating and exporting the configuration bundle daily to an SCP or FTP server, see “Scheduling Configuration Exports” .

Table 2. Configuration Management Functions (Continued)

Function	Description
Export device state (firewall only)	<p>This feature is used to export the configuration and dynamic information from a firewall that is configured as a GlobalProtect Portal with the large scale VPN feature enabled. If the Portal experiences a failure, the export file can be imported to restore the Portal's configuration and dynamic information.</p> <p>The export contains a list of all satellite devices managed by the Portal, the running configuration at the time of the export, and all certificate information (Root CA, Server, and Satellite certificates).</p> <p>Important: You must manually run the device state export or create a scheduled XML API script to export the file to a remote server. This should be done on a regular basis since satellite certificates may change often.</p> <p>To create the device 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 device 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, see the XML API Usage Guide.</p>
Import named config snapshot	Imports a configuration file from any network location. Click Browse and select the configuration file to be imported.
Import device state (firewall only)	Import the device state information that was exported using the Export device state option. This includes the current running config, Panorama templates, and shared policies. If the device is a Global Protect Portal, the export includes the Certificate Authority (CA) information and the list of satellite devices and their authentication information.
Device Operations	
Reboot	<p>To restart the firewall/Panorama, click Reboot Device. You are logged out and the PAN-OS software and active configuration are reloaded. Existing sessions will also be closed and logged and a system log entry will be created that will show the administrator name that initiated the shutdown. Any configuration changes that have not been saved or committed are lost (see “Defining Operations Settings”).</p> <p>Note: If the web interface is not available, use the CLI command <code>request restart system</code>. See the PAN-OS Command Line Interface Reference Guide for details.</p>

Table 2. Configuration Management Functions (Continued)

Function	Description
Shutdown	<p>To perform a graceful shutdown of the firewall/Panorama, click Shutdown Device or Shutdown Panorama and then click Yes on the confirmation prompt. Any configuration changes that have not been saved or committed are lost. All administrators will be logged off and the following processes will occur:</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 device will powered off. <p>You need to unplug the power source and plug it back in before you can power on the device.</p> <p><i>Note: If the web interface is not available, use the CLI command request shutdown system. See the PAN-OS Command Line Interface Reference Guide for details.</i></p>
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 and on Panorama.</p> <p><i>Note: If the web interface is not available, use the CLI command request restart dataplane. See the PAN-OS Command Line Interface Reference Guide for details.</i></p>
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 (web interface) header image • PDF Report Title Page image. See “Managing PDF Summary Reports”. • PDF Report Footer image <p>Click  to upload an image file,  to preview an image, or  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 “Managing PDF Summary Reports”.</p>
SNMP Setup	Specify SNMP parameters. See “ SNMP ”.

Table 2. Configuration Management Functions (Continued)

Function	Description
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 for a statistical report to be sent, click the report icon  . The Report Sample tab opens to display the report code. To view a report, click the check box next to the desired report, then click the Report Sample tab.</p>

Defining Hardware Security Modules

► *Device > Setup > HSM*

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

Table 3. HSM Module Provider Status settings

Field	Description
Provider Configured	<p>Indicates the vendor of the HSM connected to the firewall:</p> <ul style="list-style-type: none"> • None—The firewall does not connect to any HSM. • SafeNet Luna SA (SafeNet Network) • Thales nShield Connect <p>The HSM server version must be compatible with the HSM client version on the firewall</p>
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	See “ SafeNet Network Hardware Security Module Status settings ” or “ Thales Nshield Connect Hardware Security Module Status settings ” as required.

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

Table 4. HSM Configuration Settings

Field	Description
Provider Configured	Select the HSM vendor: <ul style="list-style-type: none"> • None—By default, the firewall does not connect to any HSM. • SafeNet Luna SA (SafeNet Network)—The SafeNet Network HSM server version must be compatible with client version 5.2.1, which runs on the firewall. • Thales nShield Connect—The Thales nShield Connect server version must be compatible with client version 11.62, which runs 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 check box if you are configuring the HSM modules in a high availability configuration. The module name and server address of each HSM module must be configured.
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 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	Configure the IPv4 address of the remote filesystem used in the Thales Nshield Connect HSM configuration.
Thales Nshield Connect Only	

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

Table 5. Setup Hardware Security Module settings

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

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

Table 6. SafeNet Network Hardware Security Module Status settings

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

Table 7. Thales Nshield Connect Hardware Security Module Status settings

Field	Description
Name	The Server name of the HSM.
IP address	The IP address of the HSM that was assigned on the firewall.
Module State	The current operating state of the HSM. <ul style="list-style-type: none"> • Authenticated • Not Authenticated

SNMP

► *Device > Setup > Operations*

Simple Network Management Protocol (SNMP) is a standard facility for monitoring the devices on your network. Use this page to configure the firewall to use the SNMP version (SNMPv2c and SNMPv3) supported by your network management station.

To configure the server profile that enables the firewall to communicate with the SNMP trap destinations on your network, see “[Configuring SNMP Trap Destinations](#)”. The SNMP Management Information Bases (MIBs) module defines all SNMP traps generated by the system. The 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** on the **Setup** page, and specify the following settings to allow SNMP GET requests from your network management station:

Table 8. SNMP Setup

Field	Description
Physical Location	Specify the physical location of the firewall. When a log or trap is generated, this information allows you to identify the device that generated the notification.
Contact	Enter the name or email address of the person responsible for maintaining the firewall. This setting is reported in the standard system information MIB.
Use Specific Trap Definitions	Select the check box to use a unique OID for each SNMP trap based on the event type (default is selected).

Table 8. SNMP Setup (Continued)

Field	Description
Version	<p>Select the SNMP version (V2c or V3). This setting controls access to the MIB information. By default, V2c is selected with the “public” community string.</p> <ul style="list-style-type: none"> • For V2c, configure the following setting: <ul style="list-style-type: none"> – SNMP Community String—Enter the SNMP community string for firewall access (default public). SNMP Community strings is required for SNMPv2c. SNMPv3 uses username/password authentication, along with an encryption key. • For V3, configure the following settings: <ul style="list-style-type: none"> – Views— Views allow you to limit which MIB objects an SNMP manager can access. Click Add and configure the following settings: <ul style="list-style-type: none"> – Name—Specify a name for a group of views. – View—Specify a name for a view. – OID—Specify the object identifier (OID) (for example, 1.2.3.4). – Option—Choose whether the OID is to be included or excluded from the view. – Mask—Specify a mask value for a filter on the OID in hexadecimal format (for example, 0xf0). – Users—Click Add and configure the following settings: <ul style="list-style-type: none"> – Users—Specify a user name. – View—Specify the group of views for the user. – Auth Password—Specify the user’s authentication password (minimum 8 characters, maximum of 256 characters, and no character restrictions). All characters allowed). Only Secure Hash Algorithm (SHA) is supported. – Priv Password—Specify the user’s encryption password (minimum 8 characters, maximum of 256 characters, and no character restrictions). Only Advanced Encryption Standard (AES) is supported.

Defining Services Settings

► *Device > Setup > Services*

The **Services** tab displays sections for **Services** and **Services Features**. Use these sections to setup the services that the firewall uses to operate efficiently:

- Use the **Services** section to define settings for Domain Name System (DNS), update servers, and proxy servers. Use the dedicated NTP tab in the Services section to configure Network Time Protocol (NTP) settings. See Table 9 for field descriptions of the options available in the **Services** section.
- Use the **Service Features** section to select or customize a Service Route Configuration. Specify how the firewall will communicate with other servers/devices for services communication, such as DNS, Email, Palo Alto Updates, and NTP. Click **Service Route Configuration** in the Services Features settings to select one of the options described in Table 10.

Table 9. Services Settings

Function	Description
Services	
DNS	Select the type of DNS service. This setting is used for all DNS queries initiated by the firewall in support of FQDN address objects, logging, and device management. Options include: <ul style="list-style-type: none"> • Primary and secondary DNS servers for domain name resolution • DNS proxy that has been configured on the firewall
Primary DNS Server	Enter the IP address of the primary DNS server. The server is used for DNS queries from the firewall, for example, to find the update server, to resolve DNS entries in logs, or for FDQN-based address objects.
Secondary DNS Server	Enter the IP address of a secondary DNS server to use if the primary server is unavailable (optional).
Update Server	This setting represents the IP address or host name of the server used to download updates from Palo Alto Networks. The current value is updates.paloaltonetworks.com . Do not change the server name unless instructed by technical support.
Verify Update Server Identity	If this option is enabled, the firewall or Panorama will verify that the server from which the software or content package is download has an SSL certificate signed by a trusted authority. This option adds an additional level of security for the communication between the firewall/Panorama server and the update server.
Proxy Server section	
Server	If the device needs to use a proxy server to reach Palo Alto Networks update services, enter the IP address or host name of the server.
Port	Enter the port for the proxy server.
User	Enter the user name to access the server.
Password/Confirm Password	Enter and confirm the password for the user to access the proxy server.
NTP	
NTP Server Address	Enter the IP address or hostname of an NTP server that you want to use to synchronize the firewall's clock. Optionally enter the IP address or hostname of a second NTP server to synchronize the firewall's clock with if the primary server becomes unavailable.

Table 9. Services Settings (Continued)

Function	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.

Table 10. Services Features

Feature	Description
Service Route Configuration	
Use Management Interface for all	This option will force all firewall service communications with external servers through the management interface (MGT). If this option is selected, you will need to configure the MGT interface to allow communications between the firewall and the servers/devices that provide services. To configure the MGT interface, navigate to Device > Setup > Management and edit the Management Interface Settings section.

Table 10. Services Features (Continued)

Feature	Description
Customize	<p>Choose this option to configure granular control for service communication using a specific source interface and IP address. 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.</p> <ul style="list-style-type: none"> • IPv4/IPv6—On either the IPv4 or IPv6 tabs, select from the list of available services and select the Source Interface and Source Address from the drop-down list. 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 the destination address since the destination is configured when configuring the given service. For example, when you define your DNS servers from the Device > Setup > Services tab that will set the destination for DNS queries. • Destination—If a service that you want to route is not listed in the Service column, you can define the Source Interface and Source Address that will be used by the service. Services not listed include items such as Kerberos, LDAP, and Panorama log collector communications. You do not need to enter the subnet for the destination address. <p>In multi-tenant environments, destination IP-based service routes will be required where common services require different source address. For example, if two tenants need to use RADIUS.</p> <p>It is important that routing and policies are setup properly for the interface that will be used to route the service. For example, if you want to route Kerberos authentication requests on an interface other than the MGT port, you need to configure the Destination and Source Address in the right section of the Service Route Configuration window since Kerberos is not listed in the default Service column. As an example, you could have a source IP address 192.168.2.1 on Ethernet1/3 and then a destination for a Kerberos server of 10.0.0.240. You will need to add Ethernet1/3 to an existing virtual router with a default route, or you can create a new virtual router from Network > Virtual Routers and add static routes as needed. This will ensure that all traffic on the interface will be routed through the virtual router to reach the appropriate destinations. In this case, the destination address is 10.0.0.240 and Ethernet1/3 interface has the source IP 192.168.2.1/24.</p> <p>The CLI output for the Destination and Source Address would look like the following:</p> <pre>PA-200-Test# show route destination { 10.0.0.240 { source address 192.168.2.1/24 } }</pre> <p>With this configuration, all traffic on interface Ethernet1/3 will use the default route defined in the virtual router and will be sent to 10.0.0.240.</p>

Defining Content-ID Settings

► *Device > Setup > Content-ID*

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

Table 11. Content-ID Settings

Function	Description
URL Filtering	
Dynamic URL Cache Timeout	Click Edit and enter the timeout (in hours). This value is used in dynamic URL filtering to determine the length of time an entry remains in the cache after it is returned from the URL filtering service. This option is applicable to URL filtering using the BrightCloud database only. For information on URL filtering, see “ URL Filtering Profiles ”.
URL Continue Timeout	Specify the interval following a user's “continue” action before the user must press continue again for URLs in the same category (range 1 - 86400 minutes, default 15 minutes).
URL Admin Override Timeout	Specify the interval 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 1 - 86400 minutes, default 900 minutes).
URL Admin Lockout Timeout	Specify the period of time that a user is locked out from attempting to use the URL Admin Override password following three unsuccessful attempts (1 - 86400 minutes, default 1800 minutes).
x-forwarded-for	<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>The system takes the value and places Src: x.x.x.x into the Source User field of the URL logs (where x.x.x.x is the IP address that is read from the header).</p>
Strip-x-forwarded-for	Remove the X-Forwarded-For header that includes the source IP address. When this option is selected, the firewall zeros out the header value before forwarding the request, and the forwarded packets do not contain internal source IP information.
Allow Forwarding of Decrypted Content	Select the check box to allow the firewall to forward decrypted content to an outside service. For example, when this option is set the firewall can send decrypted content to WildFire for analysis. For multi-VSYS configurations, this option is per VSYS.

Table 11. Content-ID Settings (Continued)

Function	Description
URL Admin Override	
Settings for URL Admin Override	<p>Specify the settings that are used when a page is blocked by the URL filtering profile and the Override action is specified. See “URL Filtering Profiles”.</p> <p>Click Add and configure the following settings for each virtual system that you want to configure for URL admin override.</p> <ul style="list-style-type: none"> • Location—Select the virtual system from the drop-down list (multi-VSYS devices only). • Password/Confirm Password—Enter the password that the user must enter to override the block page. • Server Certificate—Select the server certificate to be used with SSL communications when redirecting through the specified server. • Mode—Determines whether the block page is delivered transparently (it appears to originate at the blocked website) or redirected to the user to the specified server. If you choose Redirect, enter the IP address for redirection. <p>Click  to delete an entry.</p>
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	
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 list. 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>
Content-ID Settings	
Extended Packet Capture Length	Set the number of packets to capture when the extended-capture option is enabled in anti-spyware and vulnerability protection profiles. The range is 1-50, default is 5.

Configuring WildFire Settings

► *Device > Setup > WildFire*

Use the **WildFire** tab to configure WildFire settings on the firewall and Panorama. These settings determine whether the firewall submits files to the WildFire cloud or to a WildFire appliance. You can also set file size limits and session information that will be reported.



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

Table 12. WildFire Settings on the Firewall or Panorama

Field	Description
General Settings	
WildFire Server	<p>Specify the IP address or FQDN of a WildFire appliance or enter wildfire-public-cloud to use the WildFire cloud hosted in the United States.</p> <p>Enter <code>wildfire.paloaltonetworks.jp</code> to forward samples to the WildFire cloud hosted in Japan. You might want to use the Japan server if you do not want benign files forwarded to the U.S. cloud servers. However, if a file sent to the Japan cloud is determined to be malicious, it will be forwarded to the U.S. servers for signature generation.</p> <p>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.</p>
Maximum File Size (MB)	<p>Specify the maximum file size that will be forwarded to the WildFire server. Available ranges are:</p> <ul style="list-style-type: none"> • flash (Adobe Flash)—1-10MB, default 5MB • apk (Android Application)—1-50MB, default 10MB • pdf—(Portable Document Format) 100KB-1000KB, default 200KB • jar (Packaged Java class file)—1-10MB, default 1MB • pe (Portable Executable)—1-10MB, default 2MB • ms-office (Microsoft Office)—200KB-10000KB, default 500KB <p><i>Note: The values listed above may differ based on the version of PAN-OS and/or the content release version that is installed. To view the valid ranges, click in the Size Limit field and a pop-up will appear showing the available range and default value.</i></p>
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><i>Note: Even if this option is enabled on the firewall, email links that WildFire deems benign will not be logged because of the potential quantity of links processed.</i></p>

Table 12. WildFire Settings on the Firewall or Panorama (Continued)

Field	Description
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.

Defining Session Settings

► *Device > Setup > Session*

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

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

Session Settings

Table 13. Session Settings

Field	Description
Rematch Sessions	<p>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.</p> <p>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.</p>
ICMPv6 Token Bucket Size	Enter the bucket size for rate limiting of ICMPv6 error messages. The token bucket size is a parameter of the token bucket algorithm that controls how bursty the ICMPv6 error packets can be (range 10-65535 packets, default 100).
ICMPv6 Error Packet Rate	Enter the average number of ICMPv6 error packets per second allowed globally through the firewall (range is 10-65535 packets/second, default is 100 packets/second). This value applies to all interfaces. If the firewall reaches the ICMPv6 error packet rate, the ICMPv6 token bucket is used to enable throttling of ICMPv6 error messages.
Enable IPv6 Firewalling	<p>To enable firewall capabilities for IPv6, click Edit and select the IPv6 Firewalling check box.</p> <p>All IPv6-based configurations are ignored if IPv6 is not enabled. Even if IPv6 is enabled for an interface, the IPv6 Firewalling setting must also be enabled for IPv6 to function.</p>
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; the range is 576 to 1500 bytes. • If you check Enable Jumbo Frame, the Global MTU defaults to 9192 bytes; the range is 9192 to 9216 bytes. <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.</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.

Table 13. Session Settings (Continued)

Field	Description
NAT Oversubscription Rate	Select the DIPP NAT oversubscription rate, which is the number of times that the same translated IP address and port pair can be used concurrently. Reducing the oversubscription rate will decrease the number of source device translations, but will provide higher NAT rule capacities. <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
Accelerated Aging	Enables accelerated aging-out of idle sessions. Select the check box to enable accelerated aging and specify the threshold (%) and scaling factor. When the session table reaches the Accelerated Aging Threshold (% full), PAN-OS applies the Accelerated Aging Scaling Factor to the aging calculations for all sessions. The default scaling factor is 2, meaning that accelerated aging occurs at a rate twice as fast as the configured idle time. The configured idle time divided by 2 results in a faster timeout of one-half the time. To calculate the session's accelerated aging, PAN-OS divides the configured idle time (for that type of session) by the scaling factor to determine a shorter timeout. For example, if the scaling factor is 10, a session that would normally time out after 3600 seconds would time out 10 times faster (in 1/10 of the time), which is 360 seconds.

Session Timeouts

A session timeout defines the duration for which PAN-OS maintains a session on the firewall after inactivity in the session. By default, when the session timeout for the protocol expires, PAN-OS closes the session.

On the firewall, you can define a number of timeouts for TCP, UDP, and ICMP sessions in particular. The Default timeout applies to any other type of session. All of these timeouts are global, meaning they apply to all of the sessions of that type on the firewall.

In addition to the global settings, you have the flexibility to define timeouts for an individual application in the **Objects > Applications** tab. The timeouts available for that application appear in the Options window. The firewall applies application timeouts to an application that is in Established state. When configured, timeouts for an application override the global TCP or UDP session timeouts.

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

The defaults are optimal values. However, you can modify these according to your network needs. Setting a value too low could cause sensitivity to minor network delays and could result in a failure to establish connections with the firewall. Setting a value too high could delay failure detection.

Table 14. Session Timeouts

Field	Description
Default	Maximum length of time that a non-TCP/UDP or non-ICMP session can be open without a response. Default is 30 seconds; range is 1-15,999,999 seconds
Discard Timeouts	PAN-OS applies the discard timeout when denying a session based on security policies configured on the firewall.
– Discard Default	Applies only to non-TCP/UDP traffic. Default is 60 seconds; range is 1-15,999,999 seconds
– Discard TCP	Applies to TCP traffic. Default is 90 seconds; range is 1-15,999,999 seconds
– Discard UDP	Applies to UDP traffic. Default is 60 seconds; range is 1-15,999,999 seconds
ICMP	Maximum length of time that an ICMP session can be open without an ICMP response. Default is 6 seconds; range is 1-15,999,999 seconds
Scan	Maximum length of time that any session remains open after it is considered inactive. PAN-OS regards an application as inactive when it exceeds the trickling threshold defined for the application. Default is 10 seconds; range is 5-30 seconds
TCP	Maximum length of time that a TCP session remains open without a response, after a TCP session is in the Established state (after the handshake is complete and/or data transmission has started). Default is 3600 seconds; range is 1-15,999,999 seconds
TCP handshake	Maximum length of time between receiving the SYN-ACK and the subsequent ACK to fully establish the session. Default is 10 seconds; range is 1-60 seconds
TCP init	Maximum length of time between receiving the SYN and SYN-ACK before starting the TCP handshake timer. Default: 5 seconds; range is 1-60 seconds
TCP Half Closed	Maximum length of time between receiving the first FIN and receiving the second FIN or a RST. Default: 120 seconds; range is 1-604800 seconds
TCP Time Wait	Maximum length of time after receiving the second FIN or a RST. Default: 15 seconds; range is 1-600 seconds
Unverified RST	Maximum length of time after receiving a RST that cannot be verified (the RST is within the TCP window but has an unexpected sequence number, or the RST is from an asymmetric path). Default: 30 seconds; range is 1-600 seconds
UDP	Maximum length of time that a UDP session remains open without a UDP response. Default is 30 seconds; range is 1-1599999 seconds

Table 14. Session Timeouts (Continued)

Field	Description
Captive Portal	The authentication session timeout for the Captive Portal web form. To access the requested content, the user must enter the authentication credentials in this form and be successfully authenticated. Default is 0 seconds; range is 1-1599999 seconds To define other Captive Portal timeouts, such as the idle timer and the expiration time before the user must be re-authenticated, use the Device > User Identification > Captive Portal Settings tab. See " "Captive Portal Settings Tab" ".

Decryption Settings: Certificate Revocation Checking

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

Table 15. Session Features: Certificate Revocation Checking

Field	Description
Enable: CRL	Select this check box to use the certificate revocation list (CRL) method to verify the revocation status of certificates. If you also enable Online Certificate Status Protocol (OCSP), the firewall first tries OCSP; if the OCSP server is unavailable, the firewall then tries the CRL method. For more information on decryption certificates, see " Decryption Policies ".
Receive Timeout: CRL	If you enabled the CRL method for verifying certificate revocation status, specify the interval in seconds (1-60, default 5) after which the firewall stops waiting for a response from the CRL service.
Enable: OCSP	Select the check box to use OCSP to verify the revocation status of certificates.
Receive Timeout: OCSP	If you enabled the OCSP method for verifying certificate revocation status, specify the interval in seconds (1-60, default 5) after which the firewall stops waiting for a response from the OCSP responder.
Block Session With Unknown Certificate Status	Select the check box to block SSL/TLS sessions when the OCSP or CRL service returns a certificate revocation status of unknown. Otherwise, the firewall proceeds with the session.
Block Session On Certificate Status Check Timeout	Select the check box to block SSL/TLS sessions after the firewall registers a CRL or OCSP request timeout. Otherwise, the firewall proceeds with the session.
Certificate Status Timeout	Specify the interval in seconds (1-60, default 5) after which the firewall stops waiting for a response from any certificate status service and applies any session blocking logic you optionally define. The Certificate Status Timeout relates to the OCSP/CRL Receive Timeout as follows: <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.

Table 16. Session Features: Forward Proxy Server Certificate Settings

Field	Description
Defined by destination host	Select this option if you want PAN-OS to generate certificates based on the key that the destination server uses: <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. This is the default setting.
1024-bit RSA	Select this option if you want PAN-OS to generate certificates that use an RSA 1024-bit key and SHA-1 hashing algorithm regardless of the key size that the destination server uses. As of December 31, 2013, public certificate authorities (CAs) and popular browsers have limited support for X.509 certificates that use keys of fewer than 2048 bits. In the future, depending on its security settings, when presented with such keys the browser might warn the user or block the SSL/TLS session entirely.
2048-bit RSA	Select this option if you want PAN-OS to generate certificates that use an RSA 2048-bit key and SHA-256 hashing algorithm regardless of the key size that the destination server uses. Public CAs and popular browsers support 2048-bit keys, which provide better security than the 1024-bit keys.

Comparing Configuration Files

► *Device > Config Audit*

You can view and compare configuration files by using the **Config Audit** page. From the drop-down lists, select the configurations to compare. Select the number of lines that you want to include for context, and click **Go**. The page displays the configurations side by side in separate panes and highlights the differences line by line using colors to indicate additions (green), modifications (yellow), or deletions (red):

Added

Modified

Deleted

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

Figure 1. Configuration Comparison

Candidate Configuration	Running Configuration
<pre> ... 431 setting { 432 config { 433 rematch yes; 434 } 435 } 436 high-availability { 437 group { 438 { 439 monitoring { 440 path-monitoring { 441 path-group { 442 virtual-router { 443 default { 444 destination-ip [1.1.1.1]; 445 enabled yes; 446 failure-condition any; 447 } 448 } 449 virtual-wire { 450 default-wire { 451 enabled yes; 452 failure-condition any; 453 source-ip 2.2.2.2; 454 } 455 } 456 } 457 } 458 } 459 } 460 } 461 } 462 }</pre>	<pre> ... 431 setting { 432 config { 433 rematch yes; 434 } 435 } 436 }</pre>

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

Installing a License

► Device > Licenses

When you purchase a subscription from Palo Alto Networks, you receive an authorization code to activate one or more license keys.

The following actions are available on the **Licenses** page:

- **Retrieve license keys from license server:** To enable purchased subscriptions that require an authorization code and have been activated on the support portal, click **Retrieve license keys from license server**.
- **Activate feature using authorization code:** To enable purchased subscriptions that require an authorization code and have not been previously activated on the support portal, click **Activate feature using authorization code**. Enter your authorization code, and click **OK**.

- **Manually upload license key:** If the firewall does not have connectivity to the license server and you want to upload license keys manually, follow these steps:
 - a. Download the license key file from <http://support.paloaltonetworks.com>, and save it locally.
 - b. Click **Manually upload license key**, click **Browse** and select the file, and click **OK**.



To enable licenses for URL filtering, you must install the license, download the database, and click **Activate**. If you are using PAN-DB for URL Filtering, you will need to click **Download** to retrieve the initial seed database first and then click **Activate**.

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

If the Threat Prevention subscription on the firewall expires, the following will occur:

- A log entry will appear in the system log stating 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.

The technical support entitlement license is not tied into the threat prevention subscription. If the support license expires, threat prevention and threat prevention updates will continue to function normally. If the your support entitlement expires, operating system software updates will no longer function. You will need to renew your license to continue access to software updates and to interact with the technical support group. Contact the Palo Alto Networks operations team or sales for information on renewing your licenses/subscriptions.

Defining VM Information Sources

► *Device > VM Information Sources*

Use this tab to proactively track changes on the Virtual Machines (VMs) deployed on any of these sources— VMware ESXi server, VMware vCenter server or the Amazon Web Services, Virtual Private Cloud (AWS-VPC). There are two ways to monitor VM Information Sources:

- The firewall can monitor the VMware ESXi server, VMware vCenter server and the AWS-VPC environments and retrieve changes as you provision or modify the guests configured on the monitored sources. For each firewall or for each virtual system on a multiple virtual systems capable firewall, you can configure up to 10 sources.

If your firewalls are configured in a high availability configuration:

- in an active/passive setup, only the active firewall monitors the VM information sources.
- in an active/active setup, only the firewall with the priority value of primary monitors the VM sources.

For information on how VM Information Sources and Dynamic Address Groups can work synchronously and enable you to monitor changes in the virtual environment, see the [VM-Series Deployment Guide](#).

- For IP address to user mapping, you can either configure the VM Information Sources on the Windows User-ID agent or on the firewall to monitor the VMware ESXi and vCenter server and retrieve changes as you provision or modify the guests configured on the server. Up to 100 sources are supported on the Windows User-ID agent; support for AWS is not available for the User-ID agent.

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

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

Attributes Monitored on a VMware Source	Attributes Monitored on the AWS-VPC
<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 “[Enabling VM Information Sources for VMware ESXi or vCenter Server](#)”.
- For AWS-VPC, see “[Enabling VM Information Sources for AWS VPC](#)”.

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

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

Table 17. Enabling VM Information Sources for VMware ESXi or vCenter Server

Field	Description
Name	Enter a name to identify the monitored source (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Type	Select whether the host/source being monitored is an ESXi server or vCenter server .
Description	(Optional) Add a label to identify the location or function of the source.
Port	Specify the port on which the host/source is listening. (default port 443).
Enabled	<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 also displays as yellow when the monitored source is disabled. <p>Clear the Enabled check box 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. (default: 2 hours, range 2-10 hours)</p> <p>(Optional) To change the default value, select the check box to Enable timeout when the source is disconnected and specify the value. When the specified limit is reached or if the host is inaccessible or the host does not respond, the firewall will close the connection to the source.</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 at which the firewall retrieves information from the source. (default 5 seconds, range is 5-600 seconds)

Table 18. Enabling VM Information Sources for AWS VPC

Field	Description
Name	Enter a name to identify the monitored source (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Type	Select AWS VPC .
Description	(Optional) Add a label to identify the location or function of the source.

Table 18. Enabling VM Information Sources for AWS VPC (Continued)

Field	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 also displays as yellow when the monitored source is disabled. <p>Clear the Enabled check box to disable communication between the host and the firewall.</p>
Source	<p>Add the URI in which the Virtual Private Cloud resides. For example, ec2.us-west-1.amazonaws.com.</p> <p>The syntax is: ec2.<your_AWS_region>.amazonaws.com</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 at which the firewall retrieves information from the source. (default 60 seconds, range is 60-1200 seconds)
Timeout	<p>The interval in hours after which the connection to the monitored source is closed, if the host does not respond. (default 2 hours)</p> <p>(Optional) Select the check box to Enable timeout when the source is disconnected. When the specified limit is reached or if the source is inaccessible or the source does not respond, the firewall will close the connection to the source.</p>
VPC ID	<p>Enter the ID of the AWS-VPC to monitor, for example, vpc-1a2b3c4d. 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>

Installing the Software

► Device > Software

Use this page to install a version of the software—view the available versions, select the release you want to download and install (a support license is required), access and read the [release notes](#) for the version, [upgrade](#) or [downgrade](#) to a release.

Make sure to follow the following recommendations before upgrading or downgrading the software version:

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

- Save a backup your current configuration since a feature release may migrate certain configurations to accommodate new features. (Click **Device > Setup > Operations** tab and select **Export named configuration snapshot**, select **running-config.xml** and then click **OK** to save the configuration file to your computer.)
- When downgrading, it is recommended that you downgrade into a configuration that matches the software version.
- When upgrading a High Availability (HA) pair to a new feature release (where the first or second digit in the PAN-OS version changes, e.g. 4.1 or 5.0 to 6.0), the configuration may be migrated to accommodate new features. If session synchronization is enabled, sessions will not be synchronized if one device in the cluster is at a different PAN-OS feature release.
- The date and time settings on the firewall must be current. PAN-OS software is digitally signed and the signature is checked by the device prior to installing a new version. If the date setting on the firewall is not current, the device may perceive the software signature to be erroneously in the future and will display the message
`Decrypt failed: GnuPG edit non-zero, with code 171072 Failed to load into PAN software manager.`

The following table provides help for using this screen.

Table 19. 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	The size of the software image.
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 software image has been downloaded to the firewall.
Currently Installed	A check mark in this column indicates that the corresponding version of the software image has been activated/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 software version is available on the Palo Alto Networks Update Server. Click the link to initiate the download. If the firewall does not have access to the Internet, use an Internet-connected computer to go to the Software Update site to look for and Download the software version to your local computer. Then click the Upload button to manually upload the software image to the firewall. • Install—The corresponding software version has been downloaded to the firewall. Click the link to install the software. A reboot is required to complete the upgrade process. • Reinstall—The corresponding software version has been installed. To reinstall the same version, click the link.
Release Note	Provides a link to the release notes for the corresponding version.
	Remove the previously downloaded 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 6.1, you probably do not need the base images for 6.0 and 5.0 unless you plan on downgrading to those versions.

Updating Threat and Application Definitions

- ▶ *Device > Dynamic Updates*
- ▶ *Panorama > Dynamic Updates*

Palo Alto Networks periodically posts updates for application detection, threat protection, and GlobalProtect data files through dynamic updates for the following features:

- **Antivirus**—Includes new and updated antivirus signatures, including signatures discovered 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 get the Application and Threats update instead of the Applications update). New Applications and Threats updates are published weekly.
- **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 portal and GlobalProtect gateway license in order to receive these updates. In addition, you must create a schedule for these updates before GlobalProtect will function.
- **BrightCloud URL Filtering**—Provides updates to the BrightCloud URL Filtering database only. You must have a BrightCloud subscription to get these updates. New BrightCloud URL database updates are published daily. If you have a PAN-DB license, scheduled updates are not required as devices remain in-sync with the servers automatically.
- **WildFire**—Provides near real-time malware and antivirus signatures created as a result of the analysis done by the WildFire cloud service. Without the subscription, you must wait 24 to 48 hours for the signatures to roll into the Applications and Threat update.
- **WF-Private**—Provides near real-time malware and antivirus signatures created as a result of the analysis done by a WildFire appliance (WF-500). To receive content updates from a WF-500, the firewall and appliance must both be running PAN-OS 6.1 or later and the firewall must be configured to use the WildFire appliance for file analysis.

You can view the latest updates, read the release notes for each update, and then select the update you want to download and install. You can also revert to a previously installed version of an update.

If you are managing your firewalls using Panorama and want to schedule dynamic updates for one or more firewalls, see “[Scheduling Dynamic Updates](#)”.

The following table provides help for using this page.

Table 20. Dynamic Updates Options

Field	Description
Version	Lists the versions that are currently available on the Palo Alto Networks Update Server. To check if a new content release is available from Palo Alto Networks, click Check Now . The firewall uses the service route to connect to the Update Server and check for new versions and, if there are content updates available, displays them at the top of the list.
Last checked	Displays the date and time that the firewall last connected to the update server and checked if an update was available.
Schedule	Allows you to schedule the frequency for retrieving updates. You define how often and when the dynamic content updates occur—day or date, and time—whether the updates are downloaded only or whether the update is downloaded and installed on the firewall. When scheduling a download, if you want to delay installing new updates until it has been released for a certain number of hours, you can specify how long after a release to wait before performing a content update. Entering the number of hours to wait in the Threshold (Hours) field.
File Name	Lists the filename; it includes the content version information.
Type	Indicates whether the download is full update or an incremental update.
Size	Displays the size of the software image.
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 update has been downloaded to the firewall.
Currently Installed	A check mark in this column indicates that the corresponding content update is currently running on the firewall.
Action	Indicates the available actions for the corresponding content update as follows: <ul style="list-style-type: none"> • Download—The corresponding content release version is available on the Palo Alto Networks Update Server. Click the link to initiate the download. If the firewall does not have access to the Internet, use an Internet-connected computer to go to the Dynamic Update site to look for and Download the content update to your local computer. Then click the Upload button to manually upload the software image to the firewall. • Install—The corresponding content release version has been downloaded to the firewall. Click the link to install the update. • Revert—The corresponding content release version has been downloaded previously. To reinstall the same version, click the link.
Documentation	Provides a link to the release notes for the corresponding version.
	Remove the previously downloaded content release from the firewall.

Administrator Roles, Profiles, and Accounts

The firewall supports the following options to authenticate administrative users who attempt

to log in to the firewall:

- **Local database**—The user login and password information is entered directly into the firewall database.
- **RADIUS**—Existing Remote Authentication Dial In User Service (RADIUS) servers are used to authenticate users.
- **LDAP**—Existing Lightweight Directory Access Protocol (LDAP) servers are used to authenticate users.
- **Kerberos**—Existing Kerberos servers are used to authenticate users.
- **Client Certificate**—Existing client certificates are used to authenticate users.

When you create an administrative account, you specify local authentication or client certificate (no authentication profile), or an authentication profile (RADIUS, LDAP, Kerberos, or local DB authentication). This setting determines how the administrator's authentication is checked.

Administrator roles determine the functions that the administrator is permitted to perform after logging in. You can assign roles directly to an administrator account, or define role profiles, which specify detailed privileges, and assign those to administrator accounts.

See the following sections for additional information:

- For instructions on setting up authentication profiles, see “[Setting Up Authentication Profiles](#)”.
- For instructions on setting up role profiles, see “[Defining Administrator Roles](#)”.
- For instructions on setting up administrator accounts, see “[Creating Administrative Accounts](#)”.
- For information on SSL virtual private networks (VPNs), see “[GlobalProtect Settings](#)”.
- For instructions on defining virtual system domains for administrators, see “[Specifying Access Domains for Administrators](#)”.
- For instructions on defining certificate profiles for administrators, see “[Creating a Certificate Profile](#)”.

Defining Administrator Roles

► *Device > Admin Roles*

Use the **Admin Roles** page to define role profiles that determine the access and responsibilities available to administrative users. For instructions on adding administrator accounts, see “[Creating Administrative Accounts](#)”.

There are also three pre-defined Admin Roles that can be used for common criteria purposes. You first use the Superuser role for the initial configuration of the device and to create the administrator accounts for the Security Administrator, Audit Administrator, and Cryptographic Administrator. Once the accounts are created and the proper common criteria Admin Roles are applied, you then login using those accounts. The default Superuser account in FIPS or CC mode is **admin** and has a default password of **paloalto**. In standard operating mode, the default **admin** password is **admin**. The pre-defined Admin Roles were created

where there is no overlap in capabilities, except that all have read-only access to the audit trail (except audit administrator with full read/delete access). These admin roles cannot be modified and are defined as follows:

- **auditadmin**—The Audit Administrator is responsible for the regular review of the firewall's audit data.
- **cryptoadmin**—The Cryptographic Administrator is responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to the firewall.
- **securityadmin**—The Security Administrator is responsible for all other administrative tasks (e.g. creating the firewall's security policy) not addressed by the other two administrative roles.

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

Table 21. Administrator Role Settings

Field	Description
Name	Enter a name to identify this administrator role (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter an optional description of the role (up to 255 characters).
Role	Select the scope of administrative responsibility: device or a virtual system (for devices enabled for multi virtual system capability).
WebUI	Click the icons for specified areas to indicate the type of access permitted for the web interface: <ul style="list-style-type: none"> • Enable—Read/write access to the selected tab. • Read Only—Read only access to the selected tab. • Disable—No access to the selected tab.
XML API	Click the icons for specified areas to indicate the type of access permitted for the XML API.
Command Line	Select the type of role for CLI access: <ul style="list-style-type: none"> • None—Access to the device CLI not permitted. • superuser—Full access to the current device. • superreader—Read-only access to the current device. • deviceadmin—Full access to a selected device, except for defining new accounts or virtual systems. • devicereader—Read-only access to a selected device.

Defining Password Profiles

► *Device > Password Profiles and Panorama > Password Profiles*

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

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 “[Creating a Local User Database](#)”).

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

Table 22. Password Profile Settings

Field	Description
Name	Enter a name to identify the password profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Required Password Change Period (days)	Require that administrators change their password on a regular basis specified by the number of days set, ranging from 0-365 days. Example, if the value is set to 90, administrators will be prompted to change their password every 90 days. You can also set an expiration warning from 0-30 days and specify a grace period.
Expiration Warning Period (days)	If a required password change period is set, this setting can be used to prompt the user to change their password at each log in as the forced password change date approaches (range 0-30 days).
Post Expiration Admin Login Count	Allow the administrator to log in the specified number of times after their account has expired. Example, if the value is set to 3 and their account has expired, they can log in 3 more times before their account is locked out (range 0-3 logins).
Post Expiration Grace Period (days)	Allow the administrator to log in the specified number of days after their account has expired (range is 0-30 days).

Username and Password Requirements

The following table lists the valid characters that can be used in usernames and passwords for PAN-OS and Panorama accounts.

Table 23. Valid Characters for Usernames and Passwords

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

Creating Administrative Accounts

- ▶ *Device > Administrators*
- ▶ *Panorama > Administrators*

Administrator accounts control access to devices. A firewall administrator (**Device > Administrators**) can have full or read-only access to a single firewall or to a virtual system on a single firewall. A Panorama administrator (**Panorama > Administrators**) can have full or read-only access to Panorama and all the firewalls it manages. For more Panorama-specific details, see “[Creating Panorama Administrative Accounts](#)”. Both Panorama and individual firewalls have a predefined **admin** account that has full access.

The following authentication options are supported:

- Password authentication—The administrator enters a username and password to log in. This authentication requires no certificates. You can use it in conjunction with authentication profiles, or for local database authentication.

- Client certificate authentication (web)—This authentication requires no username or password; the certificate suffices to authenticate access to the device.
- Public key authentication (SSH)—The administrator generates a public/private key pair on the machine that requires access to the device, and then uploads the public key to the device to allow secure access without requiring the administrator to enter a username and password.



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

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

Table 24. Administrator Account Settings

Field	Description
Name	Enter a login name for the administrator (up to 15 characters). The name is case sensitive and must be unique. Use only letters, numbers, hyphens, periods, and underscores. <i>Login names cannot start with a hyphen (-).</i>
Authentication Profile	Select an authentication profile for administrator authentication. You can use this setting for RADIUS, LDAP, Kerberos, or local database authentication. For more details, see “ Setting Up Authentication Profiles ”.
Use only client certificate authentication (web)	Select the check box to use client certificate authentication for web access. If you select this check box, a username and password are not required; the certificate is sufficient to authenticate access to the device.
New Password Confirm New Password	Enter and confirm a case-sensitive password for the administrator (up to 31 characters). You can also enforce “Minimum Password” from Setup > Management .
Use Public Key Authentication (SSH)	Select the check box to use SSH public key authentication. Click Import Key and browse to select the public key file. The uploaded key appears in the read-only text area. Supported key file formats are IETF SECSH and OpenSSH. Supported key algorithms are DSA (1024 bits) and RSA (768-4096 bits). <i>Note: If the public key authentication fails, a username and password prompt is presented to the administrator.</i>

Table 24. Administrator Account Settings (Continued)

Field	Description
Role	<p>Assign a role to this administrator. The role determines what the administrator can view and modify.</p> <p>If you choose Role Based, select a custom role profile from the drop-down. For more details, see “Defining Administrator Roles” or “Defining Panorama Administrator Roles”.</p> <p>If you select Dynamic, the pre-configured roles you can select in the drop-down depend on the platform:</p> <ul style="list-style-type: none"> • Firewall: <ul style="list-style-type: none"> – Superuser—Full access to the current firewall. – Superuser (read-only)—Read-only access to the current firewall. – Device Admin—Full access to a selected firewall, except for defining new accounts or virtual systems. – Device administrator (read-only)—Read-only access to a selected firewall. – Vsys Admin—Full access to a selected virtual system on a specific firewall (if multiple virtual systems are enabled). – Vsys Admin (read-only)—Read-only access to a selected virtual system on a specific firewall. • Panorama: <ul style="list-style-type: none"> – Superuser—Full 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 administrator accounts and roles) and all device groups and templates. No access to managed firewalls.
Virtual System (Only for a firewall virtual system administrator role)	Click Add to select the virtual systems that the administrator can access.
Password Profile	Select the password profile, if applicable. To create a new password profile, see “ Defining Password Profiles ”.



On the Panorama Administrators page for “superuser,” a lock icon is shown in the right column if an account is locked out. The administrator can click the icon to unlock the account.

Specifying Access Domains for Administrators

- *Device > Access Domain*
- *Panorama > Access Domain*

Use the **Access Domain** page to specify domains for administrator access to the firewall or Panorama. The access domain is linked to RADIUS Vendor-specific Attributes (VSAs) and is supported only if a RADIUS server is used for administrator authentication. For information

on configuring RADIUS, see “[Configuring RADIUS Server Settings](#)”. For Panorama-specific information on access domains, see “[Specifying Panorama Access Domains for Administrators](#)”.

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

Table 25. Access Domain Settings

Field	Description
Name	Enter a name for the access domain (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.
Virtual Systems	Select virtual systems in the Available column and click Add to select them. <i>Access Domains are only supported on devices that support virtual systems.</i>

Setting Up Authentication Profiles

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

Use the **Authentication Profile** page to configure authentication settings that can be applied to accounts to manage access to the firewall or Panorama.

Authentication profiles specify local database, RADIUS, LDAP, or Kerberos settings and can be assigned to administrator accounts, SSL-VPN access, and captive portal. When an administrator attempts to log in to the firewall directly or through an SSL-VPN or captive portal, the firewall checks the authentication profile that is assigned to the account and authenticates the user based on the authentication settings.

If the user does not have a local administrator account, the authentication profile that is specified on the device **Setup** page determines how the user is authenticated (see “[Defining Management Settings](#)”):

- If you specify RADIUS authentication settings on the **Setup** page and the user does not have a local account on the firewall, then the firewall requests authentication information for the user (including role) from the RADIUS server. The Palo Alto Networks [RADIUS dictionary file](#) contains the attributes for the various roles.
- If **None** is specified as the authentication profile on the **Settings** page, then the user must be authenticated locally by the firewall according to the authentication profile that is specified for the user.

Table 26. Authentication Profile Settings

Field	Description
Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	<p>The scope of the authentication profile in the device context:</p> <ul style="list-style-type: none"> Template/firewall/virtual system (vsys)—For a firewall that is in Multiple Virtual System Mode, you can assign the profile to a specific vsys or select Shared to assign the profile to all the vsys on the firewall. For a firewall that is not in Multiple Virtual System Mode, the Location field does not appear in the Authentication Profile dialog, only in the Device > Authentication Profile page, where its read-only value is set to Shared. Panorama—The Location field does not appear in the Authentication Profile dialog, only in the Panorama > Authentication Profile page, where its read-only value is set to Panorama. In this context, the profile is only available to Panorama, not to the firewalls or templates that Panorama manages. <p>After you save the profile, you cannot change its Location.</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>CAUTION: If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, the Failed Attempts is ignored and the user is never locked out.</p>
Lockout Time	<p>Enter the number of minutes (0-60) for which the device locks out a user account after the user reaches the number of Failed Attempts. A value of 0 (default) means the lockout applies until an administrator manually unlocks the user account.</p> <p>CAUTION: If you set the Lockout Time to a value other than 0 but leave the Failed Attempts at 0, the Lockout Time is ignored and the user is never locked out.</p>
Allow List	<p>Specify the users and groups that are explicitly allowed to authenticate. Click Edit Allow List and do any of the following:</p> <ul style="list-style-type: none"> Select the check box next to the appropriate user or user group in the Available column, and click Add to add your selections to the Selected column. Use the All check box to apply to all users. Enter the first few characters of a name in the Search field to list all the users and user groups that start with those characters. Selecting an item in the list sets the check box in the Available column. Repeat this process as often as needed, and then click Add. To remove users or user groups, select the appropriate check boxes in the Selected column and click Remove, or select any to clear all users.

Table 26. Authentication Profile Settings (Continued)

Field	Description
Authentication	Choose the type of authentication: <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. • LDAP—Use LDAP as the authentication method. • Kerberos—Use Kerberos as the authentication method.
Server Profile	If you select RADIUS, LDAP, or Kerberos as the authentication method, choose the authentication server from the drop-down list. Servers are configured on the Server pages. See “ Configuring RADIUS Server Settings ”, “ Configuring LDAP Server Settings ”, and “ Configuring Kerberos Settings (Native Active Directory Authentication) ”.
Login Attribute	If you selected LDAP as the authentication method, enter the LDAP directory attribute that uniquely identifies the user.
Password Expiry Warning	If you are creating an authentication profile for use in authenticating GlobalProtect users and you selected LDAP as the authentication method, enter the number of days prior to password expiration to start displaying notification messages to users to alert them that their passwords are expiring in x number of days. By default, notification messages will display seven days before password expiry (range 1 day to 255 days). Users will not be able to access the VPN if their passwords expire. <p><i>Tip:</i> As a best practice, consider configuring the agents to use pre-logon connect method. This will allow users to connect to the domain to change their passwords even after the password has expired.</p> <p><i>Tip:</i> If users allow their passwords to expire, the administrator may assign a temporary LDAP password to enable users to log in to the VPN. In this workflow, it is a best practice to set the Authentication Modifier in the portal configuration to Cookie authentication for config refresh (otherwise, the temporary password will be used to authenticate to the portal, but the gateway login will fail, preventing VPN access).</p> <p>See “GlobalProtect Settings” for more details on cookie authentication and pre-logon.</p>

Creating a Local User Database

► Device > Local User Database > Users

You can set up a local database on the firewall to store authentication information for 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 “[Adding Local User Groups](#)”), you can configure authentication profiles based on the local database (see “[Setting Up Authentication Profiles](#)”).



You cannot define password profiles for administrative accounts that use local database authentication (see “[Defining Password Profiles](#)”).

Table 27. Local User Settings

Field	Description
Local User 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	Choose a virtual system or choose Shared to make the certificate available to all virtual systems.
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. Note that 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 the check box to activate the user account.

Adding Local User Groups

► *Device > Local User Database > User Groups*

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

Table 28. Local User Group Settings

Field	Description
Local User Group 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	Choose a virtual system or choose Shared to allow the user access to all available virtual systems.
All Local Users	Click Add to select the users you want to add to the group.

Configuring RADIUS Server Settings

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

Use the **RADIUS** page to configure settings for the RADIUS servers that are identified in authentication profiles. See “[Setting Up Authentication Profiles](#)”.

Table 29. RADIUS Server Settings

Field	Description
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	Choose a virtual system, or choose Shared to make the profile available to all virtual systems.
Administrator Use Only	Use this server profile for administrator authentication only.
Domain	Enter the RADIUS server domain. The domain setting is used if the user does not specify a domain when logging in.
Timeout	Enter an interval after which an authentication request times out (1-30 seconds, default 3 seconds).
Retries	Enter the number of automatic retries following a timeout before the request fails (1-5, default 3).
Retrieve User Group	Select the check box to use RADIUS VSAs to define the group that has access to the firewall.
Servers	Configure information for each server in the preferred order. <ul style="list-style-type: none"> • Name—Enter a name to identify the server. • IP address—Enter the server IP address. • Port—Enter the server port for authentication requests. • Secret/Confirm Secret—Enter and confirm a key to verify and encrypt the connection between the firewall and the RADIUS server.

Configuring LDAP Server Settings

- ▶ *Device > Server Profiles > LDAP*

► *Panorama > Server Profiles > LDAP*

Use the **LDAP** page to configure settings for the LDAP servers to use for authentication by way of authentication profiles. See “[Setting Up Authentication Profiles](#)”.

Table 30. LDAP Server Settings

Field	Description
Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	Choose a virtual system, or choose Shared to make the profile available to all virtual systems.
Administrator Use Only	Use this server profile for administrator authentication only.
Servers	Specify the host names, IP addresses, and ports of your LDAP servers.
Domain	Enter the server domain name. This domain name should be the NetBIOS name of the domain and will be added to the username when authentication is performed. For example, if your domain is paloaltonetworks.com, you only need to enter paloaltonetworks.
Type	Choose the server type from the drop-down list.
Base	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.
Bind Password/ Confirm Bind Password	Specify the bind account password. The agent saves the encrypted password in the configuration file.
SSL	Select to use secure SSL or Transport Layer Security (TLS) communications between the Palo Alto Networks device and the directory server.
Time Limit	Specify the time limit imposed when performing directory searches (1 - 30 seconds, default 30 seconds).
Bind Time Limit	Specify the time limit imposed when connecting to the directory server (1 - 30 seconds, default 30 seconds).
Retry Interval	Specify the interval after which the system will try to connect to the LDAP server after a previous failed attempt (1-3600 seconds).

Configuring Kerberos Settings (Native Active Directory Authentication)

► *Device > Server Profiles > Kerberos*

► *Panorama > Server Profiles > Kerberos*

Use the **Kerberos** page to configure Active Directory authentication without requiring customers to start Internet Authentication Service (IAS) for RADIUS support. Configuring a Kerberos server allows users to authenticate natively to a domain controller.

When the Kerberos settings are configured, Kerberos becomes available as an option when

defining authentication profiles. See “[Setting Up Authentication Profiles](#)”.

You can configure the Kerberos settings to recognize a user account in any of the following formats, where domain and realm are specified as part of the Kerberos server configuration:

- domain\username
- username@realm
- username

Table 31. Kerberos Server Settings

Field	Description
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	Choose a virtual system, or choose Shared to make the profile available to all virtual systems.
Administrator Use Only	Use this server profile for administrator authentication only.
Realm	Specify the hostname portion of the user login name (up to 127 characters) Example: The user account name <i>user@example.local</i> has realm <i>example.local</i> .
Domain	Specify the domain for the user account (up to 63 characters).
Servers	For each Kerberos server, click Add and specify the following settings: <ul style="list-style-type: none"> • Server—Enter the server IP address. • Host—Enter the server FQDN. • Port—Enter an optional port number for communication with the server.

Setting Up an Authentication Sequence

- ▶ *Device > Authentication Sequence*
- ▶ *Panorama > Authentication Sequence*

In some environments, user accounts reside in multiple directories (Local database, LDAP, RADIUS, for example). An authentication sequence is a set of authentication profiles that are applied in order when a user attempts to log in to the device (firewall or Panorama). The device will always try the local database first, and then each profile in sequence until the user is identified. Access to the device is denied only if authentication fails for any of the profiles in the authentication sequence.

Use the **Authentication Sequence** page to configure sets of authentication profiles that are tried in order when a user requests access to the device. The user is granted access if authentication is successful using any one of the authentication profiles in the sequence. For more information, see “[Setting Up Authentication Profiles](#)”.

Table 32. Authentication Sequence Settings

Field	Description
Profile Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	<p>The scope of the authentication sequence in the device context:</p> <ul style="list-style-type: none"> Template/firewall/virtual system (vsys)—For a firewall that is in Multiple Virtual System Mode, you can assign the sequence to a specific vsys or select Shared to assign the sequence to all the vsys on the firewall. For a firewall that is not in Multiple Virtual System Mode, the Location field does not appear in the Authentication Sequence dialog, only in the Device > Authentication Sequence page, where its read-only value is set to Shared. Panorama—The Location field does not appear in the Authentication Sequence dialog, only in the Panorama > Authentication Sequence page, where its read-only value is set to Panorama. In this context, the sequence is only available to Panorama, not to the firewalls or templates that Panorama manages. <p>After you save the sequence, you cannot change its Location.</p>
Lockout Time	Enter the number of minutes that a user is locked out if the number of failed attempts is reached (0-60 minutes, default 0). 0 means that the lockout is in effect until it is manually unlocked.
Failed Attempts	Enter the number of failed login attempts that are allowed before the account is locked out (1-10, default 0). 0 means that there is no limit.
Profile List	Choose the authentication profiles to include in the authentication sequence. To change the list order, select an entry and click Move Up or Move Down .

Scheduling Log Exports

► *Device > Scheduled Log Export*

You can schedule exports of logs and save them to a File Transfer Protocol (FTP) server in CSV format or use Secure Copy (SCP) to securely transfer data between the device and a remote host. Log profiles contain the schedule and FTP server information. For example, a profile may specify that the previous day's logs are collected each day at 3AM and stored on a particular FTP server.

Click **Add** and fill in the following details:

Table 33. Scheduled Log Export Settings

Field	Description
Name	<p>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.</p> <p>You cannot change the name after the profile is created.</p>
Description	Enter an optional description (up to 255 characters).
Enabled	Select the check box to enable the scheduling of log exports.

Table 33. Scheduled Log Export Settings (Continued)

Field	Description
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 the check box to use passive mode for the export. By default, this option is selected.
Username	Enter the user name for access to the FTP server. Default is anonymous.
Password / 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. <p><i>Note: 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.</i></p>

Defining Logging Destinations

Use this page to enable the firewall to record configuration changes, system events, HIP Match logs, and alarms. For each log, you can enable remote logging to Panorama (the Palo Alto Networks central management system), and generate SNMP traps, syslog messages, and email notifications.

The following table describes the remote log destinations.

Table 34. Remote Log Destinations

Destination	Description
Panorama	All log entries can be forwarded to Panorama. To specify the address of the Panorama server, see “ Defining Management Settings ”.
SNMP trap	SNMP traps can be generated by severity level for system, threat, and traffic log entries, but not for configuration log entries. To define the SNMP trap destinations, see “ Configuring SNMP Trap Destinations ”.

Syslog	Syslog messages can be generated by severity level for system, threat, traffic, and configuration log entries. To define the syslog destinations, see “Configuring Syslog Servers” .
Email	Email notifications can be sent by severity level for system, threat, traffic, and configuration log entries. To define the email recipients and servers, see “Configuring Email Notification Settings” .
<ul style="list-style-type: none">• To configure logging destinations for system logs, see “Defining System Log Settings”• To configure logging destinations for configuration logs, see “Defining Configuration Log Settings”• To configure logging destinations for HIP Match logs, see “Defining HIP Match Log Settings”• To configure logging destinations for traffic, threat and WildFire logs, see “Log Forwarding”.	

Defining Configuration Log Settings

► *Device > Log Settings > Config*

The configuration log settings specify the configuration log entries that are logged remotely with Panorama, and sent as syslog messages and/or email notifications.

Table 35. Configuration Log Settings

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

Defining System Log Settings

► *Device > Log Settings > System*

The system log settings specify the severity levels of the system log entries that are logged remotely with Panorama and sent as SNMP traps, syslog messages, and/or email notifications. The system logs show system events such as HA failures, link status changes, and administrators logging in and out.

Table 36. System Log Settings

Field	Description
Panorama	Select the check box for each severity level of the system log entries to be sent to the Panorama centralized management system. To specify the Panorama server address, see “ Defining Management Settings ”. The severity levels are: <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.

Table 36. System Log Settings (Continued)

Field	Description
SNMP Trap Email Syslog	Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the system log entries are sent. To define new destinations, see: <ul style="list-style-type: none">• "Configuring SNMP Trap Destinations".• "Configuring Syslog Servers".• "Configuring Email Notification Settings".

Defining HIP Match Log Settings

► *Device > Log Settings > HIP Match*

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

Table 37. HIP Match Log Settings

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

Defining Alarm Log Settings

► *Device > Log Settings > Alarms*

Use the Alarms page to configure notifications when a security rule (or group of rules) has been hit repeatedly in a set period of time.

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

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

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

Table 38. Alarm Log Settings

Field	Description
Enable Alarms	Enable alarms based on the events listed on this page. The Alarms button  is visible only when the Enable Alarms check box is selected.
Enable CLI Alarm Notifications	Enable CLI alarm notifications whenever alarms occur.
Enable Web Alarm Notifications	Open a window to display alarms on user sessions, including when they occur and when they are acknowledged.
Enable Audible Alarms	An audible alarm tone will play every 15 seconds on the administrator's computer when the administrator is logged into the web interface and unacknowledged alarms exist. The alarm tone will play until the administrator acknowledges all alarms. To view and acknowledge alarms, click the Alarms icon located on the bottom right of the web interface window. This feature is only available when the firewall is in CCEAL4 mode.
Encryption/Decryption Failure Threshold	Specify the number of encryption/decryption failures after which an alarm is generated.
Log DB Alarm Threshold (% Full)	Generate an alarm when a log database reaches the indicated percentage of the maximum size.
Security Policy Limits	An alarm is generated if a particular IP address or port hits a deny rule the number of times specified in the Violations Threshold setting within the period (seconds) specified in the 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.
Selective Audit	<i>Note:</i> These settings appear on the Alarms page only in Common Criteria mode. Specify the following settings: <ul style="list-style-type: none">• CC Specific Logging—Enables verbose logging required for Common Criteria (CC) compliance.• Login Success Logging—Logs the success of administrator logins to the firewall.• Login Failure Logging—Logs the failure of administrator logins to the firewall.• Suppressed Administrators—Does not generate logs for changes that the listed administrators make to the firewall configuration.

Managing Log Settings

► *Device > Log Settings > Manage Logs*

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

Configuring SNMP Trap Destinations

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

Simple Network Management Protocol (SNMP) is a standard facility for monitoring the devices on your network. In order to alert you to system events or threats on your network, monitored devices send SNMP traps to the SNMP network management stations (called SNMP trap destinations), enabling centralized alerting for all of your network devices. Use this page to configure the server profile that enables the firewall or Panorama to communicate with the SNMP trap destinations on your network. To enable SNMP GETs, see “[SNMP](#)”.

After creating the server profile that specifies how to connect to the SNMP trap destinations, you must specify which types of logs (and, for some log types, which severities) will trigger the firewall to send SNMP traps to the configured SNMP trap destinations (see “[Defining System Log Settings](#)”). In addition, in order for your SNMP management software to interpret the traps, you must install the [PAN-OS MIBs](#).

Table 39. SNMP Trap Destination Settings

Field	Description
Name	Enter a name for the SNMP profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	<p>The scope of the SNMP trap server profile in the device context:</p> <ul style="list-style-type: none"> • Template/firewall/virtual system (vsys)—For a firewall that is in Multiple Virtual System Mode, you can assign the profile to a specific vsys or select Shared to assign the profile to all the vsys on the firewall. For a firewall that is not in Multiple Virtual System Mode, the Location field does not appear in the SNMP Trap Server Profile dialog, only in the Device > Server Profiles > SNMP Trap page, where its read-only value is set to Shared. • Panorama—The Location field does not appear in the SNMP Trap Server Profile dialog, only in the Panorama > Server Profiles > SNMP Trap page, where its read-only value is set to Panorama. In this context, the profile is only available to Panorama, not to the firewalls or templates that Panorama manages. <p>After you save the profile, you cannot change its Location.</p>
Version	Choose the SNMP version (V2c or V3).

Table 39. SNMP Trap Destination Settings (Continued)

Field	Description
V2c settings	If you choose V2c, configure the following settings: <ul style="list-style-type: none">• Server—Specify a name for the SNMP trap destination name (up to 31 characters).• Manager—Specify the IP address of the trap destination.• Community—Specify the community string required to send traps to the specified destination (default public).
V3 settings	If you choose V3, configure the following settings: <ul style="list-style-type: none">• Server—Specify the SNMP trap destination name (up to 31 characters).• Manager—Specify the IP address of the trap destination.• User—Specify the SNMP user.• EngineID—Specify the engine ID of the firewall. The input is a string in hexadecimal representation. The engine ID is any number between 5 to 64 bytes. When represented as a hexadecimal string this is between 10 to 128 characters (2 characters for each byte) with two additional characters for 0x that you need to use as a prefix in the input string. Each firewall has a unique engine ID, which you can get by using a MIB browser to run a GET for OID 1.3.6.1.6.3.10.2.1.1.0.• Auth Password—Specify the user's authentication password (minimum 8 characters, maximum of 256 characters, and no character restrictions). All characters allowed). Only Secure Hash Algorithm (SHA) is supported.• Priv Password—Specify the user's encryption password (minimum 8 characters, maximum of 256 characters, and no character restrictions). Only Advanced Encryption Standard (AES) is supported.



Do not delete a destination that is used in any system log settings or logging profile.

SNMP MIBs

The firewall supports the following SNMP MIBs:

- "RFC 1213: MIB-II - Support for The System Group, The Interfaces Group.
- "RFC 2863: IF-MIB - The Interfaces Group MIB
- "RFC 2790: HOST-RESOURCES-MIB - Support for hrDeviceTable and hrProcessorTable.
- "RFC 3433: ENTITY-SENSOR-MIB - Support for entPhySensorTable.
- PAN-PRODUCT-MIB
- PAN-COMMON-MIB
- PAN-TRAPS-MIB
- PAN-LC-MIB

Palo Alto Networks also provides a full set of [PAN-OS MIBs](#).

Configuring Syslog Servers

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

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

Table 40. New Syslog Server

Field	Description
Name	Enter a name for the syslog profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	<p>The scope of the Syslog server profile in the device context:</p> <ul style="list-style-type: none"> • Template/firewall/virtual system (vsys)—For a firewall that is in Multiple Virtual System Mode, you can assign the profile to a specific vsys or select Shared to assign the profile to all the vsys on the firewall. For a firewall that is not in Multiple Virtual System Mode, the Location field does not appear in the Syslog Server Profile dialog, only in the Device > Server Profiles > Syslog page, where its read-only value is set to Shared. • Panorama—The Location field does not appear in the Syslog Server Profile dialog, only in the Panorama > Server Profiles > Syslog page, where its read-only value is set to Panorama. In this context, the profile is only available to Panorama, not to the firewalls or templates that Panorama manages. <p>After you save the profile, you cannot change its Location.</p>

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).

Table 40. New Syslog Server (Continued)

Field	Description
Custom Log Format Tab	
Log Type	Click the log type to open a dialog box that allows you to specify a custom log format. In the dialog box, click a field to add it to the Log Format area. Other text strings can be edited directly in the Log Format area. Click OK to save the settings. For details on the fields that can be used for custom logs, see “ Custom Syslog Field Descriptions ”.
Escaping	Specify escape sequences. Use the Escaped characters box to list all the characters to be escaped without spaces.



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

Custom Syslog Field Descriptions

You can configure a custom log format in a Syslog Server Profile by selecting the **Custom Log Format** tab in **Device > Server Profiles > Syslog**. Click the desired log type (Config, System, Threat, Traffic, or HIP Match) and then click the fields you want to see in the logs. The tables that follow shows the meaning of each field for each log type.

Table 41. Config Fields

Field	Meaning
actionflags	A bit field indicating if the log was forwarded to Panorama. Available in PAN-OS 4.0.0 and above.
admin	User name of the Administrator performing the configuration.
after-change-detail	Details of the configuration after a change is made.
before-change-detail	Details of the configuration before a change is made.
formtted-receive_time	Time the log was received at the management plane, shown in CEF compliant time format.
cef-formatted-time_generated	Time the log was generated, shown in CEF compliant time format.
client	Client used by the Admin; Values are Web and CLI.
cmd	Command performed by the Admin; Values are add, clone, commit, delete, edit, move, rename, set, validate.
host	Host name or IP address of the client machine
path	The path of the configuration command issued. Up to 512 bytes in length.
receive_time	Time the log was received at the management plane.
result	Result of the configuration action. Values are Submitted, Succeeded, Failed, and Unauthorized.

Table 41. Config Fields

Field	Meaning
seqno	A 64bit log entry identifier incremented sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
serial	Serial number of the device that generated the log
subtype	Subtype of the Config log; Unused.
time_generated	Time the log was received on the data plane.
type	Specifies type of log; Values are traffic, threat, config, system and hip-match.
vsys	Virtual System associated with the configuration log.

Table 42. System Fields

Field	Meaning
actionflags	A bit field indicating if the log was forwarded to Panorama. Available in PAN-OS 4.0.0 and above.
cef-formatted-receive_time	Time the log was received at the management plane, shown in CEF compliant time format.
cef-formatted-time_generated	Time the log was generated, shown in CEF compliant time format.
eventid	String showing the name of the event
fmt	Detailed description of the event. Length is up to 512 bytes.
module	This field is valid only when the value of the Subtype field is general; It provides additional information about the sub-system generating the log. Values are general, management, auth, ha, upgrade, chassis.
number-of-severity	Severity level as an integer - informational-1, low-2, medium-3, high-4, critical-5.
object	Name of the object associated with the system log.
opaque	Detailed description of the event. Length is up to 512 bytes.
receive_time	Time the log was received at the management plane
seqno	A 64bit log entry identifier that increments sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
serial	Serial number of the device that generated the log
severity	Severity associated with the event; Values are informational, low, medium, high, critical
subtype	Subtype of the system log. Refers to the system daemon generating the log; Values are crypto, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn.
time_generated	Time the log was received on the data plane.

Table 42. System Fields

Field	Meaning
type	Specifies type of log; Values are traffic, threat, config, system and hip-match.
vsys	Virtual System associated with the system event

Table 43. Threat Fields

Field	Meaning
action	Action taken for the session; Values are alert, allow, deny, drop, drop-all-packets, reset-client, reset-server, reset-both, block-url. See Action Field table below for meaning of each value.
actionflags	A bit field indicating if the log was forwarded to Panorama. Available in PAN-OS 4.0.0 and above.
app	Application associated with the session.
category	For URL Subtype, it is the URL category; for WildFire subtype, it is the verdict on the file and is either "malicious" or "benign"; for other subtypes, the value is "any".
cef-formatted-receive_time	Time the log was received at the management plane, shown in CEF compliant time format.
cef-formatted-time_generated	Time the log was generated, shown in CEF compliant time format.
contenttype	Content type of the HTTP response data. Maximum length 32 bytes. Applicable only when Subtype is URL. Available in PAN-OS 4.0.0 and above.
direction	Indicates the direction of the attack, 'client-to-server' or 'server-to-client'.
dport	Destination port utilized by the session.
dst	Original session destination IP address.
dstloc	Destination country or Internal region for private addresses. Maximum length is 32 bytes. Available in PAN-OS 4.0.0 and above.
dstuser	User name of the user to which the session was destined.
flags	32 bit field that provides details on the session; See Flags Field table for meaning of each value.
from	Zone the session was sourced from.
inbound_if	Interface that the session was sourced from.
logset	Log Forwarding Profile that was applied to the session.
misc	The actual URI when the subtype is URL; File name or file type when the subtype is file; and File name when the subtype is virus; File name when the subtype is wildfire. Length is 63 characters in PAN-OS versions before 4.0. From version 4.0, it is variable length with a maximum of 1023 characters.
natdport	Post-NAT destination port.

Table 43. Threat Fields (Continued)

Field	Meaning
natdst	If Destination NAT performed, the post-NAT Destination IP address.
natsport	Post-NAT source port.
natsrc	If Source NAT performed, the post-NAT Source IP address.
number-of-severity	Severity level as an integer - informational-1, low-2, medium-3, high-4, critical-5.
outbound_if	Interface that the session was destined to.
proto	IP protocol associated with the session.
receive_time	Time the log was received at the management plane.
repeatcnt	Number of logs with same Source IP, Destination IP, and Threat ID seen within 5 seconds; Applies to all Subtypes except URL.
rule	Name of the rule that the session matched.
seqno	A 64bit log entry identifier that increments sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
serial	Serial number of the device that generated the log.
sessionid	An internal numerical identifier applied to each session.
severity	Severity associated with the threat; Values are informational, low, medium, high, critical.
sport	Source port utilized by the session.
src	Original session source IP address.
srcloc	Source country or Internal region for private addresses. Maximum length is 32 bytes. Available in PAN-OS 4.0.0 and above.
srcuser	User name of the user that initiated the session.
subtype	Subtype of threat log; Values are URL, virus, spyware, vulnerability, file, scan, flood, data, and wildfire.
threatid	Palo Alto Networks identifier for the threat. It is a description string followed by a numerical identifier in parenthesis for some Subtypes. The numerical identifier is a 64-bit number from PAN-OS 5.0 and later.
time_generated	Time the log was generated on the data plane.
time_received	Time the log was received on the data plane.
to	Zone the session was destined to.
type	Specifies type of log; Values are traffic, threat, config, system and hip-match.
vsys	Virtual System associated with the session.
wildfire	Logs generated by WildFire.

Table 44. Traffic Fields

Field	Meaning
action	Action taken for the session; Values are allow or deny. See Action Field table.
actionflags	A bit field indicating if the log was forwarded to Panorama. Available from PAN-OS 4.0.0.
app	Application associated with the session.
bytes	Number of total bytes (transmit and receive) for the session.
bytes_received	Number of bytes in the server-to-client direction of the session. Available from PAN-OS 4.1.0 on all models except the PA-4000 series.
bytes_sent	Number of bytes in the client-to-server direction of the session. Available from PAN-OS 4.1.0 on all models except the PA-4000 series.
category	URL category associated with the session (if applicable).
cef-formatted-receive_time	Time the log was received at the management plane, shown in CEF compliant time format.
cef-formatted-time_generated	Time the log was generated, shown in CEF compliant time format.
dport	Destination port utilized by the session.
dst	Original session destination IP address.
dstloc	Destination country or Internal region for private addresses. Maximum length is 32 bytes. Available in PAN-OS 4.0.0 and above.
dstuser	User name of the user to which the session was destined.
elapsed	Elapsed time of the session.
flags	32 bit field that provides details on session; See Flags Field table for meaning of each value. This field can be decoded by AND-ing the values with the logged value.
from	Zone the session was sourced from.
inbound_if	Interface that the session was sourced from.
logset	Log Forwarding Profile that was applied to the session.
natdport	Post-NAT destination port.
natdst	If Destination NAT performed, the post-NAT Destination IP address.
natsport	Post-NAT source port.
natsrc	If Source NAT performed, the post-NAT Source IP address.
outbound_if	Interface that the session was destined to.
packets	Number of total packets (transmit and receive) for the session.
pkts_received	Number of server-to-client packets for the session. Available from PAN-OS 4.1.0 on all models except the PA-4000 series.
pkts_sent	Number of client-to-server packets for the session. Available from PAN-OS 4.1.0 on all models except the PA-4000 series.

Table 44. Traffic Fields (Continued)

Field	Meaning
proto	IP protocol associated with the session.
receive_time	Time the log was received at the management plane.
repeatcnt	Number of sessions with same Source IP, Destination IP, Application, and Subtype seen within 5 seconds; Used for ICMP only.
rule	Name of the rule that the session matched.
seqno	A 64bit log entry identifier incremented sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
serial	Serial number of the device that generated the log.
session_end_reason	<p>The reason a session terminated. If the termination had multiple causes, this field displays only the highest priority reason. The possible session end reason values are as follows, in order of priority (where the first is highest):</p> <ul style="list-style-type: none"> • threat—The firewall detected a threat associated with a reset, drop or block (IP address) action. • policy-deny—The session matched a security policy with a deny or drop action. • tcp-rst-from-client—The client sent a TCP reset to the server. • tcp-rst-from-server—The server sent a TCP reset to the client. • resources-unavailable—The session dropped because of a system resource limitation. For example, the session could have exceeded the number of out-of-order packets allowed per flow or the global out-of-order packet queue. • tcp-fin—One host or both hosts in the connection sent a TCP FIN message to close the session. • tcp-reuse—A session is reused and the firewall closes the previous session. • decoder—The decoder detects a new connection within the protocol (such as HTTP-Proxy) and ends the previous connection. • aged-out—The session aged out. • unknown—This value applies in the following situations: <ul style="list-style-type: none"> – For logs generated in a PAN-OS release that does not support the session end reason field (releases older than 6.1), the value will be <i>unknown</i> after an upgrade to the current PAN-OS release or after the logs are loaded onto the firewall. – In Panorama, logs received from firewalls for which the PAN-OS version does not support session end reasons will have a value of <i>unknown</i>.
sessionid	An internal numerical identifier applied to each session.
sport	Source port utilized by the session.
src	Original session source IP address.
srcloc	Source country or Internal region for private addresses. Maximum length is 32 bytes. Available in PAN-OS 4.0.0 and above.

Table 44. Traffic Fields (Continued)

Field	Meaning
srcuser	User name of the user that initiated the session.
start	Time of session start.
subtype	Subtype of traffic log; Values are start, end, drop, and deny. See Subtype Field table for meaning of each value.
time_generated	Time the log was generated on the data plane.
time_received	Time the log was received on the data plane.
to	Zone the session was destined to.
type	Specifies type of log; Values are traffic, threat, config, system and hip-match.
vsys	Virtual System associated with the session.

Table 45. HIP Match Fields

Field	Meaning
actionflags	A bit field indicating if the log was forwarded to Panorama. Available in PAN-OS 4.0.0 and above.
cef-formatted-receive_time	Time the log was received at the management plane, shown in CEF compliant time format.
cef-formatted-time_generated	Time the log was generated, shown in CEF compliant time format.
machinename	Name of the Users machine.
matchname	Name of the HIP Object or Profile.
matchtype	Specifies whether the HIP field represents a HIP Object or a HIP Profile.
receive_time	Time the log was received at the management plane.
repeatcnt	Number of times the HIP profile matched.
seqno	A 64bit log entry identifier incremented sequentially. Each log type has a unique number space. Available in PAN-OS 4.0.0 and above.
serial	Serial number of the device that generated the log.
src	IP address of the source user.
srcuser	User name of the Source user.
subtype	Subtype of hip-match log; Unused.
time_generated	Time the log was generated on the data plane.
type	Specifies type of log; Values are traffic, threat, config, system and hip-match.
vsys	Virtual System associated with the HIP Match log.

Configuring Email Notification Settings

- *Device > Server Profiles > Email*
- *Panorama > Server Profiles > Email*

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

Table 46. Email Notification Settings

Field	Description
Name	Enter a name for the email settings (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	<p>The scope of the email server profile in the device context:</p> <ul style="list-style-type: none"> • Template/firewall/virtual system (vsys)—For a firewall that is in Multiple Virtual System Mode, you can assign the profile to a specific vsys or select Shared to assign the profile to all the vsys on the firewall. For a firewall that is not in Multiple Virtual System Mode, the Location field does not appear in the Email Server Profile dialog, only in the Device > Server Profiles > Email page, where its read-only value is set to Shared. • Panorama—The Location field does not appear in the Email Server Profile dialog, only in the Panorama > Server Profiles > Email page, where its read-only value is set to Panorama. In this context, the profile is only available to Panorama, not to the firewalls or templates that Panorama manages. <p>After you save the profile, you cannot change its Location.</p>
Servers Tab	
Server	Enter a name to identify the server (1-31 characters). This field is just a label and does not have to be the host name of an existing SMTP server.
Display Name	Enter the name shown in the From field of the email.
From	Enter the From email address, such as “security_alert@company.com”.
To	Enter the email address of the recipient.
Additional Recipient	Optionally, enter the email address of another recipient. You can only add one additional recipient. To add multiple recipients, add the email address of a distribution list.
Gateway	Enter the IP address or host name of the Simple Mail Transport Protocol (SMTP) server used to send the email.
Custom Log Format Tab	
Log Type	Click the log type to open a dialog box that allows you to specify a custom log format. In the dialog box, click a field to add it to the Log Format area. Click OK to save the settings.
Escaping	Include escaped characters and specify the escape character or characters.



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

Configuring Netflow Settings

- *Device > Server Profiles > Netflow*

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 “[Configuring a Firewall Interface](#)”), the firewall exports NetFlow data for all traffic on that interface to the specified servers.

Table 47. Netflow Settings

Field	Description
Name	Enter a name for the Netflow server profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Template Refresh Rate	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 (1-60, default 5). Set the frequency based on how often you want the NetFlow collector to update traffic statistics.
PAN-OS Field Types	Export PAN-OS specific fields for App-ID and User-ID 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).

Using Certificates

► *Device > Certificate Management > Certificates*

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

- “[Managing Device Certificates](#)”: Use the **Device > Certificate Management > Certificates > Device Certificates** tab to manage—generate, import, renew, delete, revoke—the device certificates used for ensuring secure communication. You can also export and import the HA key that is used to secure the connection between the HA peers on the network.
- “[Managing the Default Trusted Certificate Authorities](#)”: Use the **Device > Certificate Management > Certificates > Default Trusted Certificate Authorities** tab to view, enable, and disable the certificate authorities (CAs) that the firewall trusts.
- “[Creating a Certificate Profile](#)”: Use the **Device > Certificate Management > Certificate Profile** tab to
- “[Adding an OCSP Responder](#)”

Managing Device Certificates

- ▶ *Device > Certificate Management > Certificates > Device Certificates*
- ▶ *Panorama > Certificate Management > Certificates*

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

Use this tab to generate security certificates for the following uses:

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

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

The firewall has a large list of existing trusted CAs. The trusted root CA certificate is for additional CAs that are trusted for your enterprise but are not part of the pre-installed trusted list.

- **SSL Exclude**—This certificate excludes connections if they are encountered during SSL forward proxy decryption.
- **Certificate for Secure Web GUI**—This certificate authenticates users for access to the firewall web interface. If this check box is selected for a certificate, the firewall will use this certificate for all future web-based management sessions following the next commit operation.
- **Certificate for Secure Syslog**—This certificate enables secure forwarding of syslogs to an external syslog server.

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

Table 48. Settings to Generate a Certificate

Field	Description
Certificate Name	Enter a name (up to 31 characters) to identify the certificate. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. Only the name is required.
Common Name	Enter the IP address or FQDN that will appear on the certificate.
Location	Choose a virtual system or choose Shared to make the certificate available to all virtual systems.

Table 48. Settings to Generate a Certificate (Continued)

Field	Description
Signed By	A certificate can be signed by a CA certificate that has been imported into the firewall or it can be self-signed whereby the firewall itself is the CA. If you are using Panorama, you also have the option of generating a self-signed certificate for Panorama. If you have imported CA certificates or have issued them on the device itself (self-signed), the drop down includes the CAs available to sign the certificate that is being created. To generate a Certificate Signing Request, select External Authority (CSR) . The certificate and the key pair will be generated; You can now export the CSR.
Certificate Authority	If you want the firewall to issue the certificate, select the Certificate Authority check box Marking this certificate as a CA allows you to use this certificate to sign other certificates on the firewall.
OCSP Responder	Select an OCSP responder profile from the drop-down list. The OCSP Responder profile is configured in the Device > Certificate Management > OCSP Responder tab. When you select an OCSP responder, the corresponding host name appears in the certificate.
Number of Bits	Choose the key length for the certificate. If firewall is in FIPS/CC mode, the RSA keys generated must be 2048 bits or larger
Digest	Choose the digest algorithm for the certificate. If firewall is in FIPS/CC mode, the certificate signatures must be SHA256 or higher.
Expiration (days)	Specify the number of days that the certificate will be valid. The default is 365 days. If you specify a Validity Period in a GlobalProtect Portal Satellite configuration, that value will override the value entered in this field.
Certificate Attributes	Optionally click Add to specify additional Certificate Attributes to use to identify the entity to which you are issuing the certificate. You can add any of the following attributes: Country , State , Locality , Organization , Department , Email . In addition, you can specify one of the following Subject Alternative Name fields: Host Name (SubjectAltName:DNS), IP (SubjectAltName:IP), and Alt Email (SubjectAltName:email). <i>Note: To add a country as a certificate attribute, select Country from the Type column and then click into the Value column to see the ISO 6366 Country Codes.</i>

If you have configured an HSM, the private keys are stored on the external HSM storage instead of being stored on the firewall itself.

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

Table 49. Other Supported Actions

Actions	Description
Delete	Select the certificate to delete and click Delete .
Revoke	Select the certificate that you want to revoke, and click Revoke . The certificate will be instantly set to the revoked status. No commit is required.
Renew	<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 Open 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 fill in the following details</p> <ul style="list-style-type: none"> – A name to identify the certificate. – Browse to the certificate file. If importing a PKCS #12 certificate and private key, this will be the single file holding both objects. If using PEM, this will be the public certificate only – Select the file format for the certificate file. – Select the Private key resides on Hardware Security Module check box if you are using an HSM to store the private key for this certificate. For more details on HSM, see “Defining Hardware Security Modules”. – Select the Import Private Key check box to load the private key and enter the passphrase twice. If using the PKCS #12, the key file was selected above. If using PEM, browse to the encrypted private key file (generally named *.key). – Select the virtual system to which you want to import the certificate from the drop-down list.
Generate	See generate .
Export	<p>To export a certificate, select the certificate you want to export and click Export. Choose the file format you would like the exported certificate to use (.pfx for PKCS#12 or .pem for base64 encoded format).</p> <p>Select the Export Private Key check box and enter a passphrase twice to export the private key in addition to the certificate.</p>
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.
	To export keys for HA, click Export HA Key and specify a location to save the file.
Define the usage of the certificate	In the Name column, select the link for the certificate and select the check boxes to indicate how you plan to use the certificate. For a description of each, see uses .

Managing the Default Trusted Certificate Authorities

- *Device > Certificate Management > Certificates > Default Trusted Certificate Authorities*

Use this page to view, disable, or export, the pre-included certificate authorities (CAs) that the firewall trusts. For each CA, the name, subject, issuer, expiration date and validity status is displayed.

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

Table 50 Trusted Certificate Authorities Settings

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

Creating a Certificate Profile

- *Device > Certificate Management > Certificate Profile*
- *Panorama > Certificate Management > Certificate Profiles*

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

Table 51. Certificate Profile Settings

Page Type	Description
Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	<p>The scope of the certificate profile in the device context:</p> <ul style="list-style-type: none"> Template/firewall/virtual system (vsys)—For a firewall that is in Multiple Virtual System Mode, you can assign the profile to a specific vsys or select Shared to assign the profile to all the vsys on the firewall. For a firewall that is not in Multiple Virtual System Mode, the Location field does not appear in the Certificate Profile dialog, only in the Device > Certificate Management > Certificate Profile page, where its read-only value is set to Shared. Panorama—The Location field does not appear in the Certificate Server Profile dialog, only in the Panorama > Certificate Management > Certificate Profile page, where its read-only value is set to Panorama. In this context, the profile is only available to Panorama, not to the firewalls or templates that Panorama manages. <p>After you save the profile, you cannot change its Location.</p>
Username Field	<p>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 User-ID:</p> <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	<p>Click Add and select a CA Certificate to assign to the profile. Optionally, if the firewall uses Open Certificate Status Protocol (OCSP) to verify certificate revocation status, configure the following fields to override the default behavior. For most deployments, these fields do not apply.</p> <ul style="list-style-type: none"> By default, the firewall uses the OCSP responder URL that you set in the procedure “Adding an OCSP Responder”. To override that setting, enter a Default OCSP URL (starting with <code>http://</code> or <code>https://</code>). By default, the firewall uses the certificate selected in the CA Certificate field to validate OCSP responses. To use a different certificate for validation, select it in the OCSP Verify CA Certificate field.
Use CRL	Select the check box to use a certificate revocation list (CRL) to verify the revocation status of certificates.
Use OCSP	Select the check box to use OCSP to verify the revocation status of certificates.
	<p><i>Note:</i> 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.</p>

Table 51. Certificate Profile Settings (Continued)

Page Type	Description
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 the check box 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 the check box if you want the firewall to block sessions after it registers an OCSP or CRL request timeout. Otherwise, the firewall proceeds with the session.

Adding an OCSP Responder

► *Device > Certificate Management > OCSP Responder*

Use the **OCSP Responder** page to define an Online Certificate Status Protocol (OCSP) responder (server) to verify the revocation status of certificates.

Besides adding an OCSP responder, enabling OCSP requires the following tasks:

- Enable communication between the firewall and the OCSP server: select **Device > Setup > Management**, edit the Management Interface Settings section, select **HTTP OCSP**, then click **OK**.
- If the firewall will decrypt outbound SSL/TLS traffic, optionally configure it to verify the revocation status of destination server certificates: select **Device > Setup > Sessions**, click **Decryption Certificate Revocation Settings**, select **Enable** in the OCSP section, enter the **Receive Timeout** (the interval after which the firewall stops waiting for an OCSP response), then click **OK**.
- Optionally, to configure the firewall itself 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**, 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, then click **OK** and **Commit**.

Table 52 OCSP Responder Settings

Field	Description
Name	Enter a name to identify the responder (up to 31 characters). The name is case-sensitive. It must be unique and use only letters, numbers, spaces, hyphens, and underscores.
Location	If the firewall supports multiple virtual systems, the dialog displays a Location drop-down. Select the virtual system where the responder will be available or select Shared to enable availability on all the virtual systems.
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 itself as an OCSP responder, the host name must resolve to an IP address in the interface that the firewall uses for OCSP services.

Encrypting Private Keys and Passwords on the Firewall

- ▶ *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 “[Defining Hardware Security Modules](#)”).

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:

Table 53. Master Key and Diagnostics Settings

Field	Description
Current Master Key	Specify the current master key if one exists.
New Master Key	To change the master key, enter a 16-character string and confirm the new key.
Confirm Master Key	

Table 53. Master Key and Diagnostics Settings (Continued)

Field	Description
Life Time	Specify the number of Days and Hours after which the master key expires (range 1–730 days). Warning: 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 .
Time for Reminder	Enter the number of Days and Hours before the master key expires when the firewall generates an expiration alarm. The firewall automatically opens the System Alarms dialog to display the alarm. 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. Warning: To ensure the expiration alarm displays, select Device > Log Settings , edit the Alarm Settings, and Enable Alarms .
Stored on HSM	Check this box if the master key is encrypted on a Hardware Security Module (HSM). You cannot use HSM on a dynamic interface such as a DHCP client or PPPoE. The HSM configuration is not synchronized between peer devices in high availability mode. Therefore, each peer in an HA pair can connect to a different HSM source. If you are using Panorama and would like to keep the configuration on both peers in sync, use Panorama templates to configure the HSM source on the managed firewalls. HSM is not supported on the PA-200, PA-500 and PA-2000 Series firewalls.
Common Criteria	In Common Criteria mode, additional buttons are available to run a cryptographic algorithm self-test and software integrity self-test. A scheduler is also included to specify the times at which the two self-tests will run.

Enabling HA on the Firewall

► *Device > High Availability*

For redundancy, deploy your Palo Alto Networks next-generation firewalls in a [high availability](#) configuration. There are two HA deployments:

- **active/passive**—In this deployment, the active peer continuously synchronizes its configuration and session information with the passive peer over two dedicated interfaces. In the event of a hardware or software disruption on the active firewall, the passive firewall becomes active automatically without loss of service. Active/passive HA deployments are supported with all interface modes: virtual-wire, Layer 2 or Layer 3.
- **active/active**—In this deployment, both HA peers are active and processing traffic. Such deployments are most suited for scenarios involving asymmetric routing or in cases where you want to allow dynamic routing protocols (OSPF, BGP) to maintain active status across both peers. Active/active HA is supported only in the virtual-wire and Layer 3 interface modes. In addition to the HA1 and HA2 links, active/active deployments require a dedicated HA3 link. HA3 link is used as packet forwarding link for session setup and asymmetric traffic handling.



In an HA pair, both firewalls 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.

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

Table 54. HA Settings

Field	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 the active-primary (set Device ID to 0) or active-secondary (set the Device ID to 1). • Enable Config Sync—Select this check box to enable synchronization of configuration settings between the peers. As a best practice, config sync should always be enabled. • Peer HA1 IP Address—Enter the IP address of the HA1 interface of the peer firewall. • Backup Peer HA1 IP Address—Enter the IP address for the peer's backup control link.
Active/Passive Settings	<ul style="list-style-type: none"> • Passive Link State—Choose from the following options: <ul style="list-style-type: none"> – auto—Causes the link status to reflect physical connectivity, but discards all packets received. This option allows the link state of the interface to stay up until a failover occurs, decreasing the amount of time it takes for the passive device to take over. This option is supported in Layer 2, Layer 3, and Virtual Wire mode. The auto option is desirable, if it is feasible for your network. <p> When set to auto, the link state on the passive peer in a VM-Series firewall configured as an HA pair displays in a down state on Network > Interfaces > Ethernet. The link state for the interface icon is red.</p> <ul style="list-style-type: none"> – 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—Specify the length of time (minutes) that a firewall will spend in the non-functional state before becoming passive. This timer is used only when the failure reason is a link or path monitor failure (range 1 to 60, default 1).

Table 54. HA Settings (Continued)

Field	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 0-255) when the preemptive capability is enabled on both firewalls in the pair. • Preemptive—Enable the higher priority firewall to resume active operation after recovering from a failure. The Preemption option must be enabled on both devices for the higher priority firewall to resume active operation upon recovery following a failure. If this setting is off, then the lower priority firewall remains active even after the higher priority firewall recovers from a failure. • Heartbeat Backup—Uses the management ports on the HA devices to provide a backup path for heartbeat and hello messages. The management port IP address will be shared with the HA peer through the HA1 control link. No additional configuration is required. • 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 device (in active/passive mode) or the active-secondary device (in active/active mode) will wait before taking over as the active or active-primary device after communications with the HA peer have been lost. This hold time will begin only after the peer failure declaration has been made. > Hello Interval—Enter the number of milliseconds between the hello packets sent to verify that the HA program on the other firewall is operational. The range is 8000-60000 ms with a default of 8000 ms for all platforms. > Heartbeat Interval—Specify how frequently the HA peers exchange heartbeat messages in the form of an ICMP ping (range 1000-60000 ms, default 1000 ms). > Maximum No. of Flaps—A flap is counted when the firewall leaves the active state within 15 minutes after it last left the active state. You can specify the maximum number of flaps that are permitted before the firewall is determined to be suspended and the passive firewall takes over (range 0-16, default 3). The value 0 means there is no maximum (an infinite number of flaps is required before the passive firewall takes over). > Preemption Hold Time—Enter the time a passive or active-secondary device will wait before taking over as the active or active-primary device (range 1-60 min, default 1 min).

Table 54. HA Settings (Continued)

Field	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 0-60000 ms, default 0 ms).› Additional Master Hold Up Time (min)—This time interval is applied to the same event as Monitor Fail Hold Up Time (range 0-60000 ms, default 500 ms). The additional time interval is applied only to the active device in active/passive mode and to the active-primary device in active/active mode. This timer is recommended to avoid a failover when both devices experience the same link/path monitor failure simultaneously.

Table 54. HA Settings (Continued)

Field	Description
Control Link (HA1)/Control Link (HA1 Backup)	<p>The recommended configuration for the HA control link connection is to use the dedicated HA1 link 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 devices that do not have a dedicated HA port, such as the PA-200, you should configure the management port for the Control Link HA connection and a data port interface configured with type HA for the Control Link HA1 Backup connection. Since the management port is being used in this case, there is no need to enable the Heartbeat Backup option in the Elections Settings page because the heartbeat backups will already occur through the management interface connection.</p> <p> <i>When using a data port for the HA control link, you should be aware that since the control messages have to communicate from the dataplane to the management plane, if a failure occurs in the dataplane, HA control link information cannot communicate between devices and a failover will occur. It is best to use the dedicated HA ports, or on devices that do not have a dedicated HA port, use the management port.</i></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. • Note: <i>The management port can also be used as the control link.</i> • IPv4/IPv6 Address—Enter the IPv4 or IPv6 address of the HA1 interface for the primary and backup HA1 interfaces. The backup setting is optional. • Netmask—Enter the network mask for the IP address (such as “255.255.255.0”) for the primary and backup HA1 interfaces. The backup setting is optional. • Gateway—Enter the IP address of the default gateway for the primary and backup HA1 interfaces. The backup setting is optional. • Link Speed (Models with dedicated HA ports only)—Select the speed for the control link between the firewalls for the dedicated HA1 port. • Link Duplex (Models with dedicated HA ports only)—Select a duplex option for the control link between the firewalls for the dedicated HA1 port. • Encryption Enabled—Enable encryption after exporting the HA key from the HA peer and importing it onto this device. The HA key on this device must also be exported from this device and imported on the HA peer. Configure this setting for the primary HA1 interface. The key import/export is done on the Certificates page. See “Importing, Exporting and Generating Security Certificates” on page 60. • Monitor Hold Time (ms)—Enter the length of time (milliseconds) that the firewall will wait before declaring a peer failure due to a control link failure (1000-60000 ms, default 3000 ms). This option monitors the physical link status of the HA1 port(s).

Table 54. HA Settings (Continued)

Field	Description
Data Link (HA2)	<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 in the HA pair are in the same subnet, the Gateway field should be left blank. • Enable Session Synchronization—Enable synchronization of the session information with the passive firewall, and choose a transport option. • Transport—Choose one of the following transport options: <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). • Link Speed (Models with dedicated HA ports only)—Select the speed for the control link between the active and passive firewalls for the dedicated HA2 port. • Link Duplex (Models with dedicated HA ports only)—Select a duplex option for the control link between the active and passive firewalls for the dedicated HA2 port. • HA2 keep-alive—Select this check box to monitor the health of the HA2 data link between HA peers. This option is disabled by default and you can enable it on one or both peers. If enabled, the peers will use keep-alive messages to monitor the HA2 connection to detect a failure based on the Threshold you set (default is 10000 ms). If you enable HA2 keep-alive, the HA2 Keep-alive recovery Action will be taken. Select one of the following Action settings: <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 are, state synchronization will be turned off. If the HA2 path recovers, an informational log will be generated. – Split Datapath—Select this option in active/active HA deployments to instruct each peer to take ownership of their local state and session tables when it detects an HA2 interface failure. Without HA2 connectivity, no state and session synchronization can happen; this action allows separate management of the session tables to ensure successful traffic forwarding by each HA peer. To prevent this condition, configure an HA2 Backup link.

Table 54. HA Settings (Continued)

Field	Description
	<ul style="list-style-type: none"> – Threshold (ms)—The duration in which keep-alive messages have failed before one of the above actions will be triggered (range 5000-60000ms, default 10000ms). <p><i>Note: When an HA2 backup link is configured, failover to the backup link will occur if there is a physical link failure. With the HA2 keep-alive option enabled, the failover will also occur if the HA keep-alive messages fail based on the defined threshold.</i></p>
Link and Path Monitoring Tab	
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 dropdown selection (the dropdown selection 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 200-60,000 milliseconds, default 200 milliseconds). • Ping Count—Specify the number of failed pings before declaring a failure (range 3-10 pings, default 10 pings).

Table 54. HA Settings (Continued)

Field	Description
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	Select the Enable check box to enable peers to forward packets over the HA3 link for session setup and for Layer 7 inspection (App-ID, Content-ID, and threat inspection) of asymmetrically routed sessions. forward packets between the HA peer that performs session setup and the HA peer that owns the session in an active/active configuration as well as for forwarding packets with asymmetric routing.
HA3 Interface	<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> <i>If the HA3 link fails, the active-secondary peer will transition to the non-functional state. To prevent this condition, configure a Link Aggregation Group (LAG) interface with two or more physical interfaces as the HA3 link. Active/active deployments do not support an HA3 Backup link. An aggregate interface with multiple interfaces will provide additional capacity and link redundancy to support packet forwarding between HA peers.</i></p> <p> <i>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.</i></p>
VR Sync	<p>Force synchronization of all virtual routers configured on the HA devices. Virtual Router synchronization can be used when the virtual router is not employing dynamic routing protocols. Both devices must be connected to the same next-hop router through a switched network and must use only static routing.</p>
QoS Sync	Synchronize the QoS profile selection on all physical interfaces. Use this option when both devices 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.

Table 54. HA Settings (Continued)

Field	Description
Tentative Hold Time (sec)	When a firewall in an HA active/active state fails it will go into a tentative state. This timer defines how long it will stay in this state. During the tentative period the firewall will attempt to build routing adjacencies and populate its route table before it will process any packets. Without this timer, the recovering firewall would enter the active-secondary state immediately and would blackhole packets because it would not have the necessary routes (default 60 seconds).
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 device receives the first packet, it will forward all packets requiring Layer 7 inspection to the active-primary firewall over the HA3 link.
Session Setup	<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 ownership based on the parity of the source IP address. • IP Hash—Distributes session ownership based on a hash of the source IP address or source and destination IP address, and hash seed value if you need more randomization. • First Packet—The firewall that receives the first packet performs session setup, even in cases where the peer owns the session. This option minimizes traffic over the HA3 link and ensures that the management plane-intensive work of setting up the session always happens on the firewall that receives the first packet.

Table 54. HA Settings (Continued)

Field	Description
Virtual Address	<p>Click Add, select the IPv4 or IPv6 tab and then click Add again to enter options for an HA virtual Address that will be used by the HA active/active cluster. You can select the type of virtual address to be either Floating or ARP Load Sharing. You can also mix the type of virtual address types in the cluster, 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 devices in the event of a link or device failure. You should 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 will be transitioned to the HA peer. <ul style="list-style-type: none"> – Device 0 Priority—Set the priority to determine which device will own the floating IP address. A device with the lowest value will have the highest priority. – Device 1 Priority—Set the priority to determine which device will own the floating IP address. A device with the lowest value will have the highest priority. – Failover address if link state is down—Use the failover address when the link state is down on the interface. • ARP Load Sharing—Enter an IP address that will be shared by the HA pair and will provide gateway services for hosts. This option should only be used when the firewall and hosts exist on the same broadcast domain. Select the Device Selection Algorithm: <ul style="list-style-type: none"> – IP Modulo—If this option is selected, the firewall that will respond to ARP requests will be selected based on the parity of the ARP requesters IP address. – IP Hash—If this option is selected, the firewall that will respond to ARP requests will be selected based on a hash of the ARP requesters IP address.

Operational Commands

Suspend local device	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.
Toggles as Make local device functional	To place a suspended device back into a functional state, use the following operational mode CLI command: <pre>request high-availability state functional</pre> To test failover, you can either uncable the active (or active-primary) device or you can click this link to suspend the active device.

Important items to consider when configuring HA

- The subnet that is used for the local and peer IP should not be used anywhere else on the virtual router.
- The OS and Content versions should be the same on each device. A mismatch can prevent the devices in the pair from being synchronized.
- The LEDs are green on the HA ports for the active firewall and amber on the passive firewall.

- To compare the configuration of the local and peer firewalls, using the **Config Audit** tool on the **Device** tab by selecting the desired local configuration in the left selection box and the peer configuration in the right selection box.
- Synchronize the firewalls from the web interface by pressing the **Push Configuration** button located in the HA widget on the **Dashboard** tab. Note that the configuration on the device from which you push the configuration overwrites the configuration on the peer device. To synchronize the firewalls from the CLI on the active device, use the command `request high-availability sync-to-remote running-config`.



In a High Availability (HA) active/passive configuration with devices that use 10 Gigabit SFP+ ports, when a failover occurs and the active device changes to a passive state, the 10 Gigabit Ethernet port is taken down and then brought back up to refresh the port, but does not enable transmit until the device becomes active again. If you have monitoring software on the neighboring device, it will see the port as flapping because it is going down and then up again. This is different behavior than the action with other ports, such as the 1 Gigabit Ethernet port, which is disabled and still allows transmit, so flapping is not detected by the neighboring device.

HA Lite

The PA-200 and VM-Series firewalls supports a “lite” 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.

Defining Virtual Systems

► Device > Virtual Systems

Virtual systems are independent (virtual) firewall instances that can be managed separately within a physical firewall. Each virtual system can be an independent firewall with its own security policy, interfaces, and administrators; a virtual system allows you to segment the administration of all policies (security, NAT, QoS, etc.) as well as all reporting and visibility functions provided by the firewall. 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 virtual system and then define security policies that pertain only to that department. To optimize policy administration, you can maintain separate administrator accounts for overall device and network functions while creating virtual system administrator accounts that allow access to individual virtual systems. This allows the virtual system administrator in the Finance department to manage the security policies only for that department.

Networking functions including static and dynamic routing pertain to the entire firewall (and all virtual systems on it); device and network level functions are not controlled by virtual systems. For each virtual system, 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 virtual system, you must create/assign additional virtual routers and assign interfaces, VLANs, virtual wires, as needed. By default, all interfaces, zones, and policies belong to vsys1, the default virtual system.



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

When you enable multiple virtual systems, note the following:

- All items needed for policies are created and administered by a virtual systems administrator.
- Zones are objects within virtual systems. Before defining a policy or policy object, select the virtual system from the **Virtual System** drop-down list on the **Policies** or **Objects** tab.
- Remote logging destinations (SNMP, syslog, and email), as well as applications, services, and profiles, can be shared by all virtual systems or be limited to a selected virtual system.

Before you can define virtual systems, you must first enable the multiple virtual system capability on the firewall.

To enable multiple virtual system capability, on the **Device > Setup > Management** page, click the **Edit** link in the **General Settings** section, and select the **Multi Virtual System Capability** check box. This adds a **Virtual Systems** link to the side menu.

You can now open the **Virtual Systems** tab, click **Add**, and specify the following information.

Table 55. Virtual System Settings

Field	Description
ID	Enter an integer identifier for the virtual system. See the data sheet for your firewall platform for information on the number of supported virtual systems.
Name	Enter a name (up to 31 characters) to identify the virtual system. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. Only the name is required.
General Tab	Select a DNS proxy profile from the drop-down list if you want to apply DNS proxy rules to this interface. See " DNS Proxy ". To include objects of a particular type, select the check box for that type (interface, VLAN, virtual wire, virtual router, or visible virtual system). Click Add and choose from the drop-down list. You can add one or more objects of any type. To remove an object, select it and click Delete .
Resource Tab	Enter the following settings: <ul style="list-style-type: none"> • Sessions Limit—Maximum number of sessions allowed for this virtual system. • Security Rules—Maximum number of security rules allowed for this virtual system. • NAT Rules—Maximum number of NAT rules allowed for this virtual system. • Decryption Rules—Maximum number decryption rules allowed for this virtual system. • QoS Rules—Maximum number of QoS rules allowed for this virtual system. • Application Override Rules—Maximum number of application override rules allowed for this virtual system. • PBF Rules—Maximum number of policy based forwarding (PBF) rules allowed for this virtual system. • CP Rules—Maximum number of captive portal (CP) rules allowed for this virtual system. • DoS Rules—Maximum number of denial of service (DoS) rules allowed for this virtual system. • Site to Site VPN Tunnels—Maximum number of site-to-site VPN tunnels allowed for this virtual system. • Concurrent GlobalProtect Tunnel Mode Users—Maximum number of concurrent remote GlobalProtect users allowed for this virtual system.

Configuring Shared Gateways

► *Device > Shared Gateways*

Shared gateways allow multiple virtual systems to share a single interface for external communication (typically connected to a common upstream network such as an internet service provider). All of the virtual systems communicate with the outside world through the physical interface using a single IP address. A single virtual router is used to route traffic for all of the virtual systems through the shared gateway.

Shared gateways use Layer 3 interfaces, and at least one Layer 3 interface must be configured as a shared gateway. Communications originating in a virtual system and exiting the firewall through a shared gateway require similar policy to communications passing between two virtual systems. You could configure an ‘External vsys’ zone to define security rules in the virtual system.

Table 56. Shared Gateway Settings

Field	Description
ID	Identifier for the gateway (not used by firewall).
Name	Enter a name for the shared gateway (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. Only the name is required.
DNS Proxy	(Optional) If a DNS proxy is configured, select which DNS server(s) to use for domain name queries.
Interfaces	Select check boxes for the interfaces that the shared gateway will use.

Defining Custom Response Pages

► *Device > Response Pages*

Custom response pages are the web pages that are displayed when a user tries to access a URL. You can provide a custom HTML message that is downloaded and displayed instead of the requested web page or file.

Each virtual system can have its own custom response pages. The following table describes the types of custom response pages that support customer messages.



See Appendix A, "Custom Pages" for examples of the default response pages.

Table 57. Custom Response Page Types

Page Type	Description
Antivirus Block Page	Access blocked due to a virus infection.
Application Block Page	Access blocked because the application is blocked by a security policy.
Captive Portal Comfort Page	Page for users to verify their user name and password for machines that are not part of the domain.
File Blocking Continue Page	Page for users to confirm that downloading should continue. This option is available only if continue functionality is enabled in the security profile. See " File Blocking Profiles ".
File Blocking Block Page	Access blocked because access to the file is blocked.
GlobalProtect Portal Help Page	Custom help page for GlobalProtect users (accessible from the portal).
GlobalProtect Portal Login Page	Page for users who attempt to access the GlobalProtect portal.
GlobalProtect Welcome Page	Welcome page for users who attempt to log in to the GlobalProtect portal.
SSL Certificate Errors Notify Page	Notification that an SSL certificate has been revoked.
SSL Decryption Opt-out Page	User warning page indicating that this session will be inspected.

Table 57. Custom Response Page Types (Continued)

Page Type	Description
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	<p>Page with initial block policy that allows users to bypass the block. For example, a user who thinks the page was blocked inappropriately can click the Continue button to proceed to the page.</p> <p>With the override page, a password is required for the user to override the policy that blocks this URL. See the “URL Admin Override” section of Table 1 for instructions on setting the override password.</p>
URL Filtering Safe Search Enforcement Block Page	<p>Access blocked by a security policy with a URL filtering profile that has the Safe Search Enforcement option enabled.</p> <p>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.</p>

You can perform any of the following functions under **Response Pages**.

- To import a custom HTML response page, click the link of the page type you would like to change and then click import/export. Browse to locate the page. A message is displayed to indicate whether the import succeeded. For the import to be successful, the file must be in HTML format.
- To export a custom HTML response page, click the **Export** link for the type of page. Select whether to open the file or save it to disk, and select the check box if you want to always use the same option.
- To enable or disable the **Application Block** page or **SSL Decryption Opt-out** pages, click the **Enable** link for the type of page. Select or deselect the **Enable** check box.
- To use the default response page instead of a previously uploaded custom page, delete the custom block page and commit. This will set the default block page as the new active page.

Viewing Support Information

- ▶ *Device > Support*
- ▶ *Panorama > Support*

The support page allows you to access support related options. You can view the Palo Alto Networks contact information, view your support expiration date, and view product and security alerts from Palo Alto Networks based on the serial number of your device (firewall or Panorama appliance).

Perform any of the following functions on this page:

- **Support**—Use this section to view Palo Alto Networks support contact information, view support status for the device or activate your contract using an authorization code.

- **Production Alerts/Application and Threat Alerts**—These alerts will be retrieved from the Palo Alto Networks update servers when this page is accessed/refreshed. To view the details of production alerts, or application and threat alerts, click the alert name. Production alerts will be posted if there is a large scale recall or urgent issue related to a given release. The application and threat alerts will be posted if significant threats are discovered.
- **Links**—This section provides a link to the **Support** home page, from where you can manage your cases, and a link to register the device using your support login.
- **Tech Support File**—Use the **Generate Tech Support File** link to generate a system file that the Support group can use to help troubleshoot issues that you may be experiencing with the device. After you generate the file, click **Download Tech Support File** to retrieve it and then send it to the Palo Alto Networks Support department.



If your browser is configured to automatically open files after download, you should turn off that option so the browser downloads the support file instead of attempting to open and extract it.

- **Stats Dump File**—Use the **Generate Stats Dump File** link to generate a set of XML reports that summarizes network traffic over the last 7 days. After the report is generated, click the **Download Stats Dump File** link to retrieve the report. The Palo Alto Networks or Authorized Partner systems engineer uses the report to generate an Application Visibility and Risk Report (AVR Report). The AVR highlights what has been found on the network and the associated business or security risks that may be present and is typically used as part of the evaluation process. For more information on the AVR Report, please contact you Palo Alto Networks or Authorized Partner systems engineer.

Chapter 4

Network Settings

- “Defining Virtual Wires”
- “Configuring a Firewall Interface”
- “Configuring a Virtual Router”
- “VLAN Support”
- “DHCP Server and Relay”
- “DNS Proxy”
- “Defining Interface Management Profiles”
- “Defining Monitor Profiles”
- “Defining Zone Protection Profiles”

Defining Virtual Wires

► *Network > Virtual Wires*

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

Table 58. Virtual Wire Settings

Field	Description
Virtual Wire Name	Enter a virtual wire name (up to 31 characters). This name appears in the list of virtual wires when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Interfaces	Select two Ethernet interfaces from the displayed list for the virtual wire configuration. Interfaces are listed here only if they have the virtual wire interface type and have not been assigned to another virtual wire.

Table 58. Virtual Wire Settings (Continued)

Field	Description
Tags Allowed	Enter the tag number (0 to 4094) or range of tag numbers (tag1-tag2) for the traffic allowed on the virtual wire. A tag value of zero indicates untagged traffic (the default). Multiple tags or ranges must be separated by commas. Traffic that has an excluded tag value is dropped. Note that tag values are not changed on incoming or outgoing packets. When utilizing virtual wire subinterfaces, the Tag Allowed list will cause all traffic with the listed tags to be classified to the parent virtual wire. Virtual wire subinterfaces must utilize tags that do not exist in the parent's Tag Allowed list.
Multicast Firewalling	Select this option if you want to be able to apply security rules to multicast traffic. If this setting is not enabled, multicast traffic is forwarded across the virtual wire.
Link State Pass Through	Select this check box if you want to bring down the other port in a virtual wire when a down link state is detected. If this check box is not selected, link status is not propagated across the virtual wire.

Configuring a Firewall Interface

► *Network > Interfaces*

Use this page to configure the firewall ports. These ports allow a firewall to connect with other network devices as well as other ports within a firewall. To configure a firewall interface, select one of the following tabs:

- **Ethernet** tab: Interfaces configured in the **Ethernet** tab include tap, HA, log card (PA-7050 firewall only), decrypt mirror (PA-7050, PA-5000 Series, and PA-3000 Series firewalls only), virtual wire, Layer 2 (interface and subinterface), Layer 3 (interface and subinterface), and aggregate Ethernet. See “[Configuring an Ethernet Interface](#)”.
- **VLAN** tab: See “[Configuring a VLAN Interface](#)”.
- **Loopback** tab: See “[Configuring a Loopback Interface](#)”.
- **Tunnel** tab: See “[Configuring a Tunnel Interface](#)”.

Configuring an Ethernet Interface

► *Network > Interfaces > Ethernet*

The Ethernet interface configurations all have a base configuration and additional configuration tabs. To configure the base configuration for an Ethernet interface, click the interface name on the **Ethernet** tab and specify the following settings:

Table 59. Base Interface Settings

Field	Description
Interface Name	Choose the interface from the drop-down list. Modify the name if desired. For a virtual wire interface, PAN-OS automatically populates the interface name based on the selected Ethernet interface; you cannot edit the name.

Table 59. Base Interface Settings

Field	Description
Interface Type	Select the interface type: <ul style="list-style-type: none"> • Layer 2 • Layer 3 • Tap • Virtual Wire • Log Card (PA-7050 firewall only) • Decrypt Mirror (PA-7050, PA-5000 Series, and PA-3000 Series firewalls only) • Aggregate Ethernet
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 New to define a new profile. For details, see “Configuring Netflow Settings” . <i>Note:</i> This field does not apply to the HA, log card, decrypt mirror, or aggregate Ethernet interface types. Also, the PA-4000 Series firewall does not support this feature.
Comment	Enter an optional description of the interface.

To configure the additional configuration tabs for an Ethernet interface, see the following:

- [“Configuring a Layer 2 Ethernet Interface”](#)
- [“Configuring a Layer 3 Ethernet Interface”](#)
- [“Configuring a Layer 2 Ethernet Subinterface”](#)
- [“Configuring a Layer 3 Ethernet Subinterface”](#)
- [“Configuring a Virtual Wire Interface”](#)
- [“Configuring a Tap Interface”](#)
- [“Configuring a Log Card Interface”](#)
- [“Configuring a Decrypt Mirror Interface”](#)
- [“Configuring Aggregate Interface Groups”](#)
- [“Configuring an Aggregate Ethernet Interface”](#)
- [“Configuring an HA Interface”](#)

Configuring a Layer 2 Ethernet Interface

► *Network > Interfaces > Ethernet*

Configuring a Layer 2 Ethernet interface requires the following settings on the **Config** and **Advanced** tabs:

Table 60. Layer 2 Ethernet Interface Settings

Field	Description
Config Tab	
VLAN	Select a VLAN, or click New to define a new VLAN (see “ Configuring a VLAN Interface ”). Selecting None removes the current VLAN assignment from the subinterface. To enable switching between Layer 2 interfaces, or to enable routing through a VLAN interface, you must configure a VLAN object.
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.
Security Zone	Select a security zone for the interface, or click New to define a new zone. Selecting None removes the current zone assignment from the interface.
Advanced Tab	
Link Speed	Select the interface speed in Mbps (10, 100, or 1000) or select auto.
Link Duplex	Select whether the interface transmission mode is full-duplex (full), half-duplex (half), or negotiated automatically (auto).
Link State	Select whether the interface status is enabled (up), disabled (down), or determined automatically (auto).

Configuring a Layer 3 Ethernet Interface► *Network > Interfaces > Ethernet*

For a Layer 3 Ethernet interface, configure the settings on the following tabs:

- **Config** (required)
- **Advanced** (required)
- **IPv4** (optional)
- **IPv6** (optional)

Layer 3 Ethernet Interface Config and Advanced Subtabs

In addition to the base Ethernet interface configuration, click the interface name on the **Ethernet** tab and specify the following information under the **Config** and **Advanced** subtabs.

Table 61. Layer 3 Interface Settings: Config and Advanced Subtabs

Field	Description
Config Tab	
Virtual Router	Select a virtual router, or click New to define a new virtual router (see “ Configuring a Virtual Router ”). Selecting None removes the current virtual router assignment from the interface.
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.

Table 61. Layer 3 Interface Settings: Config and Advanced Subtabs (Continued)

Field	Description
Security Zone	Select a security zone for the interface, or click New to define a new zone. Selecting None removes the current zone assignment from the interface.
Advanced Tab	
Link Speed	Select the interface speed in Mbps (10, 100, or 1000) or select auto.
Link Duplex	Select whether the interface transmission mode is full-duplex (full), half-duplex (half), or negotiated automatically (auto).
Link State	Select whether the interface status is enabled (up), disabled (down), or determined automatically (auto).
Other Info	<ul style="list-style-type: none"> • Management Profile—Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Selecting None removes the current profile assignment from the interface. • MTU—Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576-1500, default 1500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the interface receives a packet exceeding the MTU, the firewall returns an <i>ICMP fragmentation needed</i> message to the source indicating the packet is too large. • Adjust TCP MSS—Select this check box if you want to adjust the maximum segment size (MSS) to 40 bytes less than the interface MTU. This setting addresses situations where a tunnel through the network requires a smaller MSS. If a packet cannot fit within the MSS without fragmenting, this setting enables the adjustment. • 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 OSPF uses multicast, the firewall does not support it on untagged subinterfaces.
ARP/Interface Entries	To add one or more static Address Resolution Protocol (ARP) entries, click Add , then enter an IP address and its associated hardware (media access control or 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.
ND Entries	To add a neighbor for discovery click Add , then enter the IP address and MAC address of the neighbor.

Layer 3 Ethernet Interface IPv4 Subtab

To configure a Layer 3 Ethernet interface on an IPv4 network, configure the following settings on the **IPv4** subtab:

Table 62. Layer 3 Interface Settings: IPv4 Subtab

Field/Subtab	Description
Type	<p>Select a method for defining the IP address information:</p> <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. <p><i>Note: Firewalls that are in active/active high availability (HA) mode do not support PPPoE or DHCP Client.</i></p> <p>The other fields that the tab displays depend on the type selection, as described below.</p>
Static	
IP (address table)	<p>Click Add, then perform one of the following steps to specify an 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: <i>ip_address/mask</i> (for example, 192.168.2.0/24 for IPv4 or 2001:db8::/32 for IPv6). • Select an existing address object of type IP netmask. • Select New 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>
PPPoE	
General (subtab)	<ul style="list-style-type: none"> • Enable—Select the check box 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—Optionally, click this link to open a dialog that displays parameters that the firewall negotiated with the Internet service provider (ISP) to establish a connection. The specific information depends on the ISP.

Table 62. Layer 3 Interface Settings: IPv4 Subtab (Continued)

Field/Subtab	Description
Advanced (subtab)	<ul style="list-style-type: none"> Authentication—Select the authentication protocol for PPPoE communications: CHAP (Challenge-Handshake Authentication Protocol), PAP (Password Authentication Protocol), or the default Auto (the firewall determines the protocol). Selecting None removes the current protocol assignment from the interface. Static Address—Perform one of the following steps to specify the IP address that the Internet service provider assigned (no default value): <ul style="list-style-type: none"> Type the entry in Classless Inter-domain Routing (CIDR) notation: <i>ip_address/mask</i> (for example, 192.168.2.0/24 for IPv4 or 2001:db8::/32 for IPv6). Select an existing address object of type IP netmask. Select New 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 the check box to automatically create a default route that points to the PPPoE peer when connected. Default Route Metric—For the route between the firewall and Internet service provider, enter a route metric (priority level) to associate with the default route and to use for path selection (optional, range 1-65535). The priority level increases as the numeric value decreases. Access Concentrator—Optionally, enter the name of the access concentrator on the Internet service provider end to which the firewall connects (no default). Service—Optionally, enter the service string (no default). Passive—Select the check box to use passive mode. In passive mode, a PPPoE end point waits for the access concentrator to send the first frame.
DHCP Client	
Enable	Select the check box to activate the DHCP client on the interface.
Automatically create default route pointing to default gateway provided by server	Select the check box 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 1-65535, no default). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info	Click 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).

Layer 3 Ethernet Interface IPv6 Subtab

To configure a Layer 3 Ethernet interface on an IPv6 network, configure the following settings on the **IPv6** subtab:

Table 63. Layer 3 Interface Settings: IPv6 Subtab

Field	Description
Enable IPv6 on the interface	Select the check box 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 (e.g. 2001:400:f00::1/64). You can also select an existing IPv6 address object or select New to create an address object. • Enable address on interface—Select this check box to enable the IPv6 address on the interface. • Use interface ID as host portion—Select this check box to use the Interface ID as the host portion of the IPv6 address. • Anycast—Select this check box to include routing through the nearest node. • Send Router Advertisement—Select this check box to enable router advertisement (RA) for this IP address. (You must also enable the global Enable Router Advertisement option on the interface.) For details on RA, see “Router Advertisement Section” 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 2592000. – Preferred Lifetime—The length of time (in seconds) that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new connections but any existing connections are valid until the Valid Lifetime expires. The default is 604800. – On-link—Select this check box if systems that have addresses within the prefix are reachable without a router. – Autonomous—Select this check box if systems can independently create an IP address by combining the advertised prefix with an interface ID.

Address Resolution Section

Enable Duplication Address Detection	Select the check box 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 1-10, default 1).

Table 63. Layer 3 Interface Settings: IPv6 Subtab (Continued)

Field	Description
Reachable Time	Specify the length of time (in seconds) that a neighbor remains reachable after a successful query and response (range 1-36000, default 30).
NS Interval (neighbor solicitation interval)	Specify the number of seconds for DAD attempts before failure is indicated (range 1-10, default 1).
Router Advertisement Section	
Enable Router Advertisement	To provide stateless address auto-configuration (SLAAC) on IPv6 interfaces, select the check box and configure the other fields in this section. Clients that receive the router advertisement (RA) messages use this information. RA enables the firewall to act as a default gateway for IPv6 hosts that are not statically configured and to provide the host with an IPv6 prefix for address configuration. You can use a separate DHCPv6 server in conjunction with this feature to provide DNS and other settings to clients. This option is a global setting for the interface. If you want to set RA options for individual IP addresses, click Add in the IP address table and configure the address (for details, see “ Address ” in this table). If you set RA options for any IP address, you must select the Enable Router Advertisement option for the interface.
Min Interval (sec)	Specify the minimum interval (in seconds) between RAs that the firewall will send (range 3-1350, default 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)	Specify the maximum interval (in seconds) between RAs that the firewall will send (range 4-1800, default 600). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit	Specify the hop limit to apply to clients for outgoing packets (range 1-255, default 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 1280-9192, default 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 0-3600000, default 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 0-4294967295, default unspecified).
Router Lifetime (sec)	Specify how long (in seconds) the client will use the firewall as the default gateway (range 0-9000, default 1800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
Router Preference	If the network segment has multiple IPv6 routers, the client uses this field to select a preferred router. Select whether the RA advertises the firewall router as having a High , Medium (default), or Low priority relative to other routers on the segment.

Table 63. Layer 3 Interface Settings: IPv6 Subtab (Continued)

Field	Description
Managed Configuration	Select the check box to indicate to the client that addresses are available via DHCPv6.
Other Configuration	Select the check box to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.
Consistency Check	Select the check box if you want the firewall to verify that RAs sent from other routers are advertising consistent information on the link. The firewall logs any inconsistencies.

Configuring an Ethernet Subinterface

► *Network > Interfaces > Ethernet*

The Ethernet subinterface configurations all have a base configuration and additional configuration tabs. To configure the base configuration for an Ethernet interface, click the link for the interface on the **Ethernet** tab and specify the following settings:

Table 64. Base Interface Settings

Field	Description
Interface Name	Enter a number (1-9999) to identify the subinterface.
Tag	Enter the VLAN tag (1-4094) for the subinterface.
Netflow Profile	If you want to export unidirectional IP traffic that traverses an ingress interface to a NetFlow server, select the server profile or click New to define a new profile. For details, see “ Configuring Netflow Settings ”. <i>Note: The PA-4000 Series firewall does not support this feature.</i>
Comments	Enter an optional description of the subinterface.

To configure the additional tabs for an Ethernet interface, see the following:

- “[Configuring a Layer 2 Ethernet Subinterface](#)”
- “[Configuring a Layer 3 Ethernet Subinterface](#)”

Configuring a Layer 2 Ethernet Subinterface

For each Ethernet port configured as a 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 configure the main Layer 2 interfaces, see “[Configuring a Layer 2 Ethernet Interface](#)”. To enable switching between Layer 2 subinterfaces, assign the same VLAN object to them.

To configure a Layer 2 Ethernet subinterface, configure the base Ethernet settings (see “[Configuring an Ethernet Subinterface](#)”) and the following additional information.

Table 65. Layer 2 Subinterface Settings

Field	Description
VLAN	Select a VLAN, or click New to define a new VLAN (see “ Configuring a VLAN Interface ”). Selecting None removes the current VLAN assignment from the subinterface. To enable switching between Layer 2 interfaces, or to enable routing through a VLAN interface, you must configure a VLAN object.
Security Zone	Select a security zone for the interface, or click New to define a new zone. Selecting None removes the current zone assignment from the interface.
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.

Configuring a Layer 3 Ethernet Subinterface

► *Network > Interfaces >Ethernet*

For a Layer 3 Ethernet subinterface, you must configure the base Ethernet settings (see “[Configuring an Ethernet Subinterface](#)”) and additional information on the following tabs:

- **Config** (required)
- **Advanced** (required)
- **IPv4** (optional)
- **IPv6** (optional)

Layer 3 Ethernet Subinterface Config and Advanced Subtabs

Table 66. Layer 3 Subinterface Settings: Config and Advanced subtabs

Field	Description
Config Tab	
Virtual Router	Select a virtual router, or click New to define a new virtual router (see “ Configuring a Virtual Router ”). Selecting None removes the current virtual router assignment from the subinterface.
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.
Security Zone	Select a security zone for the subinterface, or click New to define a new zone. Selecting None removes the current zone assignment from the subinterface.
Advanced Subtab	
Other Info	<ul style="list-style-type: none"> • Management Profile—Select a profile that defines the protocols (for example, SSH, Telnet, and HTTP) you can use to manage the firewall over this interface. Selecting None removes the current profile assignment from the interface. • MTU—Enter the maximum transmission unit (MTU) in bytes for packets sent on this subinterface (576-1500, default 1500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD) and the subinterface receives a packet exceeding the MTU, the firewall returns an <i>ICMP fragmentation needed</i> message to the source indicating the packet is too large. • Adjust TCP MSS—Select this check box if you want to adjust the maximum segment size (MSS) to 40 bytes less than the subinterface MTU. This setting addresses situations where a tunnel through the network requires a smaller MSS. If a packet cannot fit within the MSS without fragmenting, this setting enables the adjustment.
ARP Entries	To add one or more static Address Resolution Protocol (ARP) entries, click Add , then enter an IP address and its associated hardware (media access control or 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.
ND Entries	To add a neighbor for discovery click Add , then enter the IP address and MAC address of the neighbor.

Layer 3 Ethernet Subinterface IPv4 Subtab

To configure a Layer 3 Ethernet subinterface on an IPv4 network, you must configure the following settings on the **IPv4** subtab:

Table 67. Layer 3 Subinterface Settings: IPv4 Subtab

Field	Description
Type	<p>Select a method for defining the IP address information:</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><i>Note: Firewalls that are in active/active high availability (HA) mode do not support DHCP Client.</i></p> <p>The other fields that the tab displays depend on the type selection, as described below.</p>
Static	
IP (address table)	<p>Click Add, then perform one of the following steps to specify an IP address and network mask for the subinterface:</p> <ul style="list-style-type: none"> • Type the entry in Classless Inter-domain Routing (CIDR) notation: <i>ip_address/mask</i> (for example, 192.168.2.0/24 for IPv4 or 2001:db8::/32 for IPv6). • Select an existing address object of type IP netmask. • Select New 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>
DHCP Client	
Enable	Select the check box to activate the DHCP client on the subinterface.
Automatically create default route pointing to default gateway provided by server	Select the check box 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, enter a route metric (priority level) to associate with the default route and to use for path selection (optional, range 1-65535). The priority level increases as the numeric value decreases.
Show DHCP Client Runtime Info	Click 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).

Layer 3 Ethernet Subinterface IPv6 Subtab

To configure a Layer 3 Ethernet subinterface on an IPv6 network, you must configure the following settings on the **IPv6** subtab:

Table 68. Layer 3 Subinterface Settings: IPv6 Tab

Field	Description
Enable IPv6 on the interface	Select the check box to enable IPv6 addressing on this subinterface.

Table 68. Layer 3 Subinterface Settings: IPv6 Tab (Continued)

Field	Description
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 (e.g. 2001:400:f00::1/64). You can also select an existing IPv6 address object or select New to create an address object. • Enable address on interface—Select this check box to enable the IPv6 address on the subinterface. • Use interface ID as host portion—Select this check box to use the Interface ID as the host portion of the IPv6 address. • Anycast—Select this check box to include routing through the nearest node. • Send Router Advertisement—Select this check box to enable router advertisement (RA) for this IP address. (You must also enable the global Enable Router Advertisement option on the subinterface.) For details on RA, see “Router Advertisement Section” 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 2592000. – Preferred Lifetime—The length of time (in seconds) that the valid address is preferred, which means the firewall can use it to send and receive traffic. After the preferred lifetime expires, the firewall cannot use the address to establish new connections but any existing connections are valid until the Valid Lifetime expires. The default is 604800. – On-link—Select this check box if systems that have addresses within the prefix are reachable without a router. – Autonomous—Select this check box if systems can independently create an IP address by combining the advertised prefix with an interface ID.

Address Resolution Section

Enable Duplication Address Detection	Select the check box 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 1-10, default 1).
Reachable Time	Specify the length of time (in seconds) that a neighbor remains reachable after a successful query and response (range 1-36000, default 30).
NS Interval (neighbor solicitation interval)	Specify the number of seconds for DAD attempts before failure is indicated (range 1-10, default 1).

Table 68. Layer 3 Subinterface Settings: IPv6 Tab (Continued)

Field	Description
Router Advertisement Section	
Enable Router Advertisement	To provide stateless address auto-configuration (SLAAC) on the subinterface, select the check box and configure the other fields in this section. Clients that receive the router advertisement (RA) messages use this information.
	RA enables the firewall to act as a default gateway for IPv6 hosts that are not statically configured and to provide the host with an IPv6 prefix for address configuration. You can use a separate DHCPv6 server in conjunction with this feature to provide DNS and other settings to clients.
	This option is a global setting for the subinterface. If you want to set RA options for individual IP addresses, click Add in the IP address table and configure the address (for details, see “ Address ” in this table). If you set RA options for any IP address, you must select the Enable Router Advertisement option for the subinterface.
Min Interval (sec)	Specify the minimum interval (in seconds) between RAs that the firewall will send (range 3-1350, default 200). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Max Interval (sec)	Specify the maximum interval (in seconds) between RAs that the firewall will send (range 4-1800, default 600). The firewall will send RAs at random intervals between the minimum and maximum values you configure.
Hop Limit	Specify the hop limit to apply to clients for outgoing packets (range 1-255, default 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 1280-9192, default 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 0-3600000, default 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 0-4294967295, default unspecified).
Router Lifetime (sec)	Specify how long (in seconds) the client will use the firewall as the default gateway (range 0-9000, default 1800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
Router Preference	If the network segment has multiple 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 the check box to indicate to the client that addresses are available via DHCPv6.
Other Configuration	Select the check box to indicate to the client that other address information (for example, DNS-related settings) is available via DHCPv6.

Table 68. Layer 3 Subinterface Settings: IPv6 Tab (Continued)

Field	Description
Consistency check	Select the check box if you want the firewall to verify that RAs sent from other routers are advertising consistent information on the link. The firewall logs any inconsistencies.

Configuring a Virtual Wire Interface

► *Network > Interfaces > Ethernet*

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

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

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

Table 69. Virtual Wire Settings

Field	Description
Config Tab	
Virtual Wire	Select a virtual wire, or click New to define a new virtual wire (see “ Defining Virtual Wires ”).
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.
Security Zone	Select a security zone for the interface, or click New to define a new zone. Selecting None removes the current zone assignment from the interface.
Advanced Tab	
Link Speed	Specify the interface speed. If the selected interface is a 10 Gbps interface, the only option is auto . In other cases, the options are: 10 , 100 , 1000 , or 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).

Configuring a Virtual Wire Subinterface

► *Network > Interfaces*

Virtual wire 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 subinterface, select the virtual wire interface where you want to add the subinterface, and click **Add Subinterface** and specify the following information.

Table 70. Virtual Wire Subinterface Settings

Field	Description
Interface Name	The main interface name is automatically populated based on the interface that you selected; the label cannot be edited. To define the subinterface, enter a number (1 to 9999) to the physical interface name to form the logical interface name. The general name format is: <code>ethernetx/y.<1-9999></code> To configure the virtual wire, see “ Configuring a Virtual Wire Interface ”.
Tag	Enter the tag number (0 to 4094) of the traffic received on this interface. Setting a tag value of 0 will match untagged traffic.
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 New to define a new profile. For details, see “ Configuring Netflow Settings ”. <i>Note:</i> The PA-4000 Series firewall does not support this feature.
Comment	Enter an optional description of the interface.
IP Classifier	Click Add to add an IP address, subnet, or IP range or any combination of the IP classifiers, to classify traffic entering the firewall through this physical port into this subinterface based on its source IP address. Return-path traffic entering the firewall through the other end of the associated virtual wire will be matched according to its destination address. On a virtual wire subinterface, IP classification can only be used in conjunction with VLAN based classification.
Assign Interface To	
Security Zone	Select a security zone for the interface, or click New to define a new zone. Selecting None removes the current zone assignment from the interface.
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.
Virtual Wire	Select a virtual wire, or click New to define a new virtual wire (see “ Defining Virtual Wires ”).

Configuring a Tap Interface

► *Network > Interfaces > Ethernet*

A tap interface can be configured as required to monitor traffic on a port. In addition to the base Ethernet interface configuration, click the interface name on the **Ethernet** tab and specify the following information under the **Config** and **Advanced** tabs.

Table 71. Tap Interface Settings

Field	Description
Config Tab	
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.
Security Zone	Select a security zone for the interface, or click New to define a new zone. Selecting None removes the current zone assignment from the interface.
Advanced Tab	
Link Speed	Select the interface speed in Mbps (10, 100, or 1000) or 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).

Configuring a Log Card Interface

► *Network > Interfaces > Ethernet*

On a PA-7050 firewall, 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, SNMP and WildFire file forwarding. Only one port on the firewall can be a log card interface. If you enable log forwarding but do not configure any interface as the log card, a commit error occurs.

On the **Ethernet** tab, click the interface name, configure the base Ethernet interface information, then configure the following information under the **Log Card Forwarding** and **Advanced** tabs.

Table 72. Log Card Interface Settings

Field	Description
Log Card Forwarding	
IPv4	If your network uses IPv4, enter the following IPv4 addressing information for the port: <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, enter the following IPv6 addressing information for the port: <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.

Table 72. Log Card Interface Settings (Continued)

Field	Description
Advanced Tab	
Link Speed	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 (auto). The default is auto .
Link State	Select whether the interface status is enabled (up), disabled (down), or determined automatically (auto). The default is auto .

Configuring a Decrypt Mirror Interface

► *Network > Interfaces > Ethernet*

To use the Decryption Port Mirror feature, you must select the **Decrypt Mirror** interface type. This feature enables creating a copy of decrypted traffic from a firewall and sending it to a traffic collection tool that can receive raw packet captures—such as NetWitness or Solera—for archiving and analysis. Organizations that require comprehensive data capture for forensic and historical purposes or data leak prevention (DLP) functionality require this feature. Decryption port mirroring is only available on the PA-7050, PA-5000 Series and PA-3000 Series firewalls. To enable the feature, you must acquire and install the free license.

On the **Ethernet** tab, click the interface name, configure the base Ethernet interface information, then specify the following information in the **Advanced** tab.

Table 73. Decrypt Mirror Interface Settings

Field	Description
Link Speed	Select the interface speed in Mbps (10, 100, or 1000) or 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).

Configuring Aggregate Interface Groups

► *Network > Interfaces*

An aggregate interface group combines multiple Ethernet interfaces using IEEE 802.1AX link aggregation. You can aggregate 1Gbps or 10Gbps XFP and SFP+ Ethernet. The aggregate interface you create becomes a logical interface. The following are properties of the logical interface, not the underlying physical interfaces: configuration assignments (virtual system, virtual router, virtual wire, VLAN, security zone), IP addresses, management profile, Link Aggregation Control Protocol (LACP) configuration, Address Resolution Protocol (ARP)

entries, and Neighbor Discovery (ND) entries. Therefore, after creating the group, perform operations such as configuring Layer 2 or Layer 3 parameters on the aggregate group, not on individual interfaces.

The following rules apply to aggregate groups:

- Within a group, the 1 Gbps links must be all copper or all fiber.
- A group can have up to eight interfaces.
- Aggregate groups support HA, virtual wire, Layer 2, or Layer 3 interfaces. Within a group, all the interfaces must be the same type. PAN-OS validates this during the commit operation.
- You can use aggregate groups for redundancy and throughput scaling on the HA3 (packet forwarding) link in active/active high availability (HA) deployments. Support for HA3 is limited to the PA-500, PA-3000 Series, PA-4000 Series, and PA-5000 Series firewalls.
- If you enable LACP for an aggregate group, support is limited to HA3, Layer 2, and Layer 3 interfaces. You cannot enable LACP for virtual wire interfaces. Support for LACP-enabled groups is limited to the PA-500, PA-3000 Series, PA-4000 Series, PA-5000 Series, and PA-7050 firewalls.

To configure an aggregate group, click **Add Aggregate Group** and specify the information in the following table, then assign interfaces to the group as described in [“Configuring an Aggregate Ethernet Interface”](#).

Table 74. Aggregate Group Interface Settings

Field	Description
Interface Name	Enter a name and numeric suffix to identify the aggregate group. The name is listed as <i>mm.n</i> where <i>mm</i> is the name and <i>n</i> is the suffix (1-8).
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. No additional configuration is required. Optionally, configure LACP as described below. Virtual Wire—No additional configuration is required. This type is not available if you enable LACP. Layer 2—Configure the Config tab and, optionally, the LACP tab as described below, then configure the Advanced tab as described in Table 65. Layer 3—Configure the Config tab and, optionally, the LACP tab as described below, then configure the other tabs as described in Table 66, Table 67, and Table 68.
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 New to define a new profile. For details, see “ Configuring Netflow Settings ”. <p>Note: This field does not apply to the HA interface type. Also, the PA-4000 Series firewall does not support this feature.</p>
Comment	Enter an optional description of the interface.
Config	
Assign Interface To	The interface assignment depends on the interface type: <ul style="list-style-type: none"> HA—This type has no Config tab options to specify. Virtual Wire—Specify a Virtual Wire and Security Zone as described in Table 70. Layer 2—Specify a VLAN and Security Zone as described in Table 65. Layer 3—Specify a Virtual Router and Security Zone as described in Table 66.
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.
LACP	
This section only applies to HA (HA3 only), Layer 2, and Layer 3 interfaces.	
Enable LACP	Select this check box if you want to enable Link Aggregation Control Protocol (LACP) for the aggregate group. LACP is disabled by default.
Mode	Select the LACP mode of the firewall. Between any two LACP peers, it is recommended that one be active and the other passive. LACP cannot function if both peers are passive. <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.

Table 74. Aggregate Group Interface Settings (Continued)

Field	Description
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 check box if, when an interface goes down, you want the firewall to fail over to an operational interface within one second. Otherwise, failover occurs at the standard IEEE 802.1AX-defined speed (at least three seconds).
System Priority	The number that determines whether the firewall or its peer overrides the other with respect to port priorities (see the Max Ports field description below). Note that the lower the number, the higher the priority. The range is 1-65535 and the default is 32768.
Max Ports	The number of interfaces (1-8) that can be active at any given time in an LACP aggregate group. The value cannot exceed the number of interfaces you assign to the group. If the number of assigned interfaces exceeds the number of active interfaces, the firewall uses the port priorities of the interfaces to determine which are in standby mode. You set port priorities when configuring individual interfaces for the group.
Same System MAC Address for Active-Passive HA	Firewalls in a high availability (HA) pair have the same system priority value. However, in an active/passive deployment, the system ID for each can be the same or different, depending on whether you assign the same MAC address. When the LACP peers (also in HA mode) are virtualized (appearing to the network as a single device), using the same system MAC address for the firewalls is a best practice to minimize latency during failover. When the LACP peers are not virtualized, using the unique MAC address of each firewall is the best practice to minimize failover latency. If the firewalls are not in active/passive HA mode, PAN-OS ignores this field. (Firewalls in an active/active deployment require unique MAC addresses so PAN-OS automatically assigns them.) LACP uses the MAC address to derive a system ID for each LACP peer. If the firewall pair and peer pair have identical system priority values, LACP uses the system ID values to determine which overrides the other with respect to port priorities. If both firewalls have the same MAC address, both will have the same system ID, which will be higher or lower than the system ID of the LACP peers. If the HA firewalls have unique MAC addresses, it is possible for one to have a higher system ID than the LACP peers while the other has a lower system ID. In the latter case, when failover occurs on the firewalls, port prioritization switches between the LACP peers and the firewall that becomes active.
MAC Address	If you enabled Use Same System MAC Address , select a system-generated MAC address, or enter your own, for both firewalls in the HA pair. You must verify the address is globally unique.

Configuring an Aggregate Ethernet Interface

► *Network > Interfaces*

To configure an aggregate Ethernet interface, first add the aggregate group to which you will assign the interface (see “[Configuring Aggregate Interface Groups](#)”). Second, click the name of the interface you will assign to the aggregate group. The interface you select must be the

same type as that defined for the aggregate group, though you will change the type to **Aggregate Ethernet** when you configure it. Specify the following information for the interface.

Table 75. Aggregate Ethernet Interface Settings

Field	Description
Interface Type	Select Aggregate Ethernet .
Aggregate Group	Assign the interface to an aggregate group.
Comment	Enter an optional description of the interface.
Advanced Tab	
<p><i>Note:</i> If you enable LACP for the aggregate group, it is a best practice to set the same link speed and duplex values for every interface in that group. For non-matching values, the commit operation displays a warning and PAN-OS defaults to the higher speed and full duplex.</p>	
Link Speed	Select the interface speed in Mbps (10, 100, or 1000) or 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).
LACP Port Priority	The firewall only uses this field if you enabled Link Aggregation Control Protocol (LACP) for the aggregate group. An aggregate group might have more interfaces than it supports in active states. (In the aggregate group configuration, the Max Ports parameter determines the number of active interfaces). In this case, the port priority assigned to each interface determines whether it is active or standby. The lower the numeric value, the higher the priority. The range is 1-65535 and the default is 32768.

Configuring an HA Interface

► *Network > Interfaces*

Each HA interface has a specific function: one interface is for configuration synchronization and heartbeats and the other interface is for state synchronization. If active/active high availability is enabled, a third HA interface can be used to forward packets.



Some Palo Alto Networks firewalls include dedicated physical ports for use in HA deployments (one for the control link and one for the data link). For firewalls that do not include dedicated ports, you must specify the data ports that will be used for HA. For additional information on HA, see “[Enabling HA on the Firewall](#)”.

To define an HA interface, click an interface name and specify the following information.

Table 76. HA Interface Settings

Field	Description
Interface Name	Choose the interface from the drop-down list. Modify the name if desired.
Interface Type	Select HA from the drop-down list.
Comment	Enter an optional description of the interface.

Table 76. HA Interface Settings (Continued)

Field	Description
Advanced Tab	
Link Speed	Select the interface speed in Mbps (10, 100, or 1000) or 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).

Configuring a VLAN Interface

► *Network > Interfaces > VLAN*

A VLAN interface can be configured to provide routing into a Layer 3 network (IPv4 and IPv6). One or more Layer 2 Ethernet ports ([“Configuring a Layer 2 Ethernet Interface”](#)) can be added to a VLAN interface. The VLAN interface configurations all have a base configuration and additional configuration tabs. To configure a VLAN interface select the **VLAN** tab and click **Add**. Specify the base configuration settings first and then the IPv4 and IPv6 settings as required.

Table 77. VLAN Interface Base Configuration Settings

Field	Description
Interface Name	Specify a numeric suffix for the interface (1-4999).
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 New to define a new profile. For details, see “Configuring Netflow Settings” . <i>Note:</i> The PA-4000 Series firewall does not support this feature.
Comment	Add an optional description of the interface.
Config Tab	
VLAN	Select a VLAN, or click New to define a new VLAN (see “Configuring a VLAN Interface”). Selecting None removes the current VLAN assignment from the subinterface.
Virtual Router	Select a virtual router, or click New to define a new virtual router (see “Configuring a Virtual Router”). Selecting None removes the current virtual router assignment from the interface.
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.
Security Zone	Select a security zone for the interface, or click New to define a new zone. Selecting None removes the current zone assignment from the interface.

Table 77. VLAN Interface Base Configuration Settings (Continued)

Field	Description
Advanced Tab	
Other Info	<p>Specify the following:</p> <ul style="list-style-type: none"> • Management Profile—Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface. • MTU—Enter the MTU in bytes for packets sent on this interface (512-1500, default 1500). If machines on either side of the firewall perform PMTUD, the MTU value will be returned in an ICMP fragmentation needed message indicating that the MTU is too large. • Adjust TCP MSS—if you select this check box, the maximum segment size (MSS) is adjusted to 40 bytes less than the interface MTU. This setting addresses the situation in which a tunnel through the network requires a smaller MSS. If a packet cannot fit within the MSS without fragmenting, this setting allows an adjustment to be made.
ARP/Interface Entries	To add one or more static ARP entries, click Add and enter an IP address and its associated hardware (MAC) address and Layer 3 interface that can access the hardware address.
ND Entries	Click Add to enter the IP address and MAC address of neighbors to add for discovery.

VLAN IPv4 Tab

If configuring a VLAN for access to an IPv4 network, you must configure the following settings on the **IPv4** tab:

Table 78. VLAN Interface IPv4 Settings

Field	Description
IPv4 Tab	
Static	Select Static to assign static IP addresses. Click Add and enter an IP address and network mask for the interface in Classless Inter-domain Routing (CIDR) notation: <i>ip_address/mask</i> (for example, 192.168.2.0/24). You can enter multiple IP addresses for the interface. The forwarding information base (FIB) your system uses determines the maximum number of IP addresses.
DHCP Client	Select DHCP to use DHCP address assignment for the interface, and specify the following: <ul style="list-style-type: none"> • Enable—Select the check box to activate the DHCP client on the interface. • Automatically create default route point to server—Select the check box to automatically create a default route that points to the DHCP server when connected. • Default Route Metric—Specify the route metric to be associated with the default route and used for path selection (optional, range 1-65535). Click Show DHCP Client Runtime Info to open a window that displays all settings received from the DHCP server, including DHCP lease status, dynamic IP assignment, subnet mask, gateway, server settings (DNS, NTP, domain, WINS, NIS, POP3, and SMTP).

Table 78. VLAN Interface IPv4 Settings (Continued)

Field	Description
ARP Entries	To add one or more static ARP entries, enter an IP address and its associated hardware (MAC) address, and click Add . To delete a static entry, select the entry and click Delete .

VLAN IPv6 Tab

If configuring a VLAN for access to an IPv6 network, you must configure the following settings on the **IPv6** tab:

Table 79. VLAN Interface IPv6 Settings

Field	Description
IPv6 Tab	
Enable IPv6 on the interface	Select the check box to enable IPv6 addressing for the subinterface.
Interface ID	Enter the 64-bit extended unique identifier in hexadecimal format, for example, 00:26:08:FF:FE:DE:4E:29. If the interface ID is left blank, the firewall will use the EUI-64 generated from the physical interface's MAC address.
Address	<p>Click Add and enter an IPv6 address and prefix length, for example 2001:400:f00::1/64. Select Use interface ID as host portion to assign an IPv6 address to the interface that will use the interface ID as the host portion of the address. Select Anycast to include routing through the nearest node. If Prefix is not selected, the IPv6 address assigned to the interface will be wholly specified in the address text box.</p> <p>Use the Send Router Advertisement (Send RA) option to enable router advertisement for this IP address. You can also set the Autonomous flag to be sent and you can set the on-link option. You must enable the global Enable Router Advertisement option on the interface before enabling Send Router Advertisement option for a specific IP address.</p>
Address Resolution (Duplicate Address Detection)	<p>Select the check box to enable Duplicate Address Detection (DAD) and specify the following information.</p> <ul style="list-style-type: none"> • DAD Attempts—Specify the number of attempts within the neighbor solicitation interval for DAD before the attempt to identify neighbors fails (range 1-10). • Reachable Time—Specify the length of time that a neighbor remains reachable after a successful query and response (range 1-36000 seconds). <p>Neighbor Solicitation (NS) Interval—Specify the number of seconds for DAD attempts before failure is indicated (range 1-10 seconds)</p>

Table 79. VLAN Interface IPv6 Settings (Continued)

Field	Description
Enable Router Advertisement	<p>Select the check box to enable Router Advertisement (RA) to provide Stateless Address Autoconfiguration (SLAAC) on IPv6 interfaces. This enables the firewall to act as a default gateway for IPv6 hosts that are not statically configured and will provide the host with an IPv6 prefix that can be used for address configuration. A separate DHCPv6 server can be used in conjunction with this feature to provide DNS and other settings to clients.</p> <p>This option is a global setting for the interface, you can also set router advertisement options per IP address by clicking Add and entering in an IP address. You must enable this option on the interface if you are going to specify the Send Router Advertisement option per address.</p> <p>Specify the following information that will be used by clients who receive the RA messages.</p> <ul style="list-style-type: none"> • Min Interval (sec)—Specify the minimum interval per second that the firewall will send out router advertisements. Router Advertisements will be sent at random intervals between the minimum and maximum values that are configured (range 3-1350 seconds, default 200 seconds). • Max Interval (sec)—Specify the maximum interval per second that the firewall will send out router advertisements. Router Advertisements will be sent at random intervals between the minimum and maximum values that are configured (range 4-1800 seconds, default 600 seconds). • Hop Limit—Specify the hop limit that will be applied to clients for outgoing packets. Enter 0 for no hop limit (range 1-255, default 64). • Link MTU—Specify the link MTU that will be applied to clients. Select unspecified for no link MTU (range 1280-9192, default unspecified). • Reachable Time (ms)—Specify the reachable time that the client will use to assume a neighbor is reachable after having received a reachability confirmation message. Select unspecified for no reachable time value (range 0-3600000 milliseconds, default unspecified). • Retrans Time (ms)—Specify the retransmission timer that the client will use to determine how long it should wait before retransmitting neighbor solicitation messages. Select unspecified for no retrans time (range 0-4294967295 milliseconds, default unspecified). • Router Lifetime (sec)—Specify the router lifetime that instructs the client on how long the firewall/router should be used as the default router (range 0-9000 seconds, default 1800). • Managed Configuration—Select the check box to indicate to the client that addresses are available via DHCPv6. • Other Configuration—Select the check box to indicate to the client that other addresses information is available via DHCPv6, such as DNS-related settings. <p>Consistency check—Select the check box to enable consistency checks that the firewall will use to verify that router advertisement sent from other routers are advertising consistent information on the link. If inconsistencies are detected, a log will be created.</p>

Configuring a Loopback Interface

► *Network > Interfaces > Loopback*

You can configure one or more loopback interfaces if your network topology requires them (IPv4 and IPv6). Loopback interface configurations all have a base configuration and additional configuration tabs. To configure a loopback interface, select **Network > Interfaces > Loopback** and click **Add**. Specify the base configuration settings first, then the advanced settings, and then the IPv4 or IPv6 settings.

Table 80. Loopback Interface Base Configuration and Advanced Settings

Field	Description
Interface Name	Specify a numeric suffix for the interface (1-4999).
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 New to define a new profile. For details, see “ Configuring Netflow Settings ”. <i>Note: The PA-4000 Series firewall does not support this feature.</i>
Comment	Add an optional description of the interface.
Config Tab	
Virtual Router	Select a virtual router, or click New to define a new virtual router (see “ Configuring a Virtual Router ”). Selecting None removes the current virtual router assignment from the interface.
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.
Security Zone	Select a security zone for the interface, or click New to define a new zone. Selecting None removes the current zone assignment from the interface.
Advanced Tab	
Other Info	<p>Specify the following settings:</p> <ul style="list-style-type: none"> • Management Profile—Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface. • MTU—Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (576 to 1500, default 1500). If machines on either side of the firewall perform Path MTU Discovery (PMTUD), the MTU value will be returned in an ICMP fragmentation needed message indicating that the MTU is too large. • Adjust TCP MSS—If you select this check box, the maximum segment size (MSS) is adjusted to 40 bytes less than the interface MTU. This setting addresses the situation in which a tunnel through the network requires a smaller MSS. If a packet cannot fit within the MSS without fragmenting, this setting allows an adjustment to be made.

Loopback Interface IPv4 Tab

If configuring a Loopback interface for access to an IPv4 network, you must configure the following settings on the **IPv4** tab:

Table 81. Loopback Interface IPv4 Settings

Field	Description
IP Address	Click Add to enter IP addresses and network masks for the interface.

Loopback Interface IPv6 Tab

If configuring a Loopback interface for access to an IPv6 network, you must configure the following settings on the **IPv6** tab:

Table 82. Loopback Interface IPv6 Settings

Field	Description
Enable IPv6 on the interface	Select the check box to enable IPv6 addressing for the subinterface.
Interface ID	Specify the unique 64-bit hexadecimal identifier for the subinterface.
Address	Enter the IPv6 address. Select Use interface ID as host portion to assign an IPv6 address to the interface that will use the interface ID as the host portion of the address. Select Anycast to include routing through the nearest node.

Configuring a Tunnel Interface► *Network > Interfaces > Tunnel*

One or more tunnel interfaces can be configured as required by your network topology (IPv4 and IPv6). The Tunnel interface configurations all have a base configuration and additional configuration tabs. To configure a Tunnel interface select the **Tunnel** tab and click **Add**. Specify the base configuration settings first followed by the IPv4 and IPv6 settings as required.

Table 83. Tunnel Interface Settings

Field	Description
Interface Name	Specify a numeric suffix for the interface (1-4999).
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 New to define a new profile. For details, see “ Configuring Netflow Settings ”. <i>Note: The PA-4000 Series firewall does not support this feature.</i>
Comment	Add an optional description of the interface.
Config Tab	
Virtual Router	Select a virtual router, or click New to define a new virtual router (see “ Configuring a Virtual Router ”). Selecting None removes the current virtual router assignment from the interface.
Virtual System	If the firewall supports multiple virtual systems (vsys) and that capability is enabled, select a vsys for the interface, or click New to define a new vsys.
Security Zone	Select a security zone for the interface, or click New to define a new zone. Selecting None removes the current zone assignment from the interface.

Table 83. Tunnel Interface Settings (Continued)

Field	Description
Advanced Tab	
Other Info	<p>Specify the following:</p> <ul style="list-style-type: none"> • Management Profile—Select a profile that specifies which protocols, if any, can be used to manage the firewall over this interface. • MTU—Enter the MTU in bytes for packets sent on this interface (512–1500, default 1500). If machines on either side of the firewall perform PMTUD, the MTU value will be returned in an ICMP fragmentation needed message indicating that the MTU is too large. <p><i>The firewall automatically considers tunnel overhead when performing IP fragmentation and also adjusts the TCP maximum segment size (MSS) as needed.</i></p>

Tunnel Interface IPv4 Tab

If configuring a tunnel interface for access to an IPv4 network, you must configure the following settings on the **IPv4** tab:

Table 84. Tunnel Interface IPv4 Settings

Field	Description
IP Address	Click Add to enter IP addresses and network masks for the interface.

Tunnel Interface IPv6 Tab

If configuring a tunnel interface for access to an IPv6 network, you must configure the following settings on the **IPv6** tab:

Table 85. Tunnel Interface IPv6 Settings

Field	Description
Enable IPv6 on the interface	<p>Select the check box to enable IPv6 addressing for the interface.</p> <p>This option allows you to route IPv6 traffic over an IPv4 IPSec tunnel and will provide confidentiality between IPv6 networks. The IPv6 traffic is encapsulated by IPv4 and then ESP.</p> <p>To route IPv6 traffic to the tunnel, you will either use a static route to the tunnel, or use a Policy Based Forwarding (PBF) rule to direct traffic and to provide redundancy by monitoring the other end of the tunnel and failing over when needed.</p>
Interface ID	Enter the 64-bit extended unique identifier in hexadecimal format, for example, 00:26:08:FF:FE:DE:4E:29. If the interface ID is left blank, the firewall will use the EUI-64 generated from the physical interface's MAC address.
Address	Click Add and enter an IPv6 address and prefix length, for example 2001:400:f00::1/64. Select Use interface ID as host portion to assign an IPv6 address to the interface that will use the interface ID as the host portion of the address. Select Anycast to include routing through the nearest node. If Prefix is not selected, the IPv6 address assigned to the interface will be wholly specified in the address text box.

Configuring a Virtual Router

► *Network > Virtual Routers*

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

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

- **Static Routes** tab: See “[Configuring the Static Routes tab](#)”.
- **Redistribution Profile** tab: See “[Configuring the Redistribution Profiles Tab](#)”.
- **RIP** tab: See “[Configuring the RIP Tab](#)”.
- **OSPF** tab: See “[Configuring the OSPF Tab](#)”.
- **OSPFv3** tab: See “[Configuring the OSPFv3 Tab](#)”.
- **BGP** tab: See “[Configuring the BGP Tab](#)”.
- **Multicast** tab: See “[Configuring the Multicast Tab](#)”.

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

- **More Runtime Stats** link: See “[More Runtime Stats for a Virtual Router](#)”.

Configuring the General tab

► *Network > Virtual Router > General*

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

Table 86. Virtual Router Settings - General Tab

Field	Description
Name	Specify a name to describe the virtual router (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Interfaces	Select the interfaces that you want to include in the virtual router. When you select an interface, it is included in the virtual router and can be used as an outgoing interface in the virtual router's routing tab. To specify the interface type, see “ Configuring a Firewall Interface ”. <i>When you add an interface, its connected routes are added automatically.</i>

Table 86. Virtual Router Settings - General Tab (Continued)

Field	Description
Administrative Distances	Specify the following administrative distances: <ul style="list-style-type: none">• Static routes (10-240, default 10).• OSPF Int (10-240, default 30).• OSPF Ext (10-240, default 110).• IBGP (10-240, default 200).• EBGP (10-240, default 20).• RIP (10-240, default 120).

Configuring the Static Routes tab

► *Network > Virtual Router > Static Routes*

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

Table 87. Virtual Router Settings - Static Routes Tab

Field	Description
Name	Enter a name to identify the static route (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Destination	Enter an IP address and network mask in Classless Inter-domain Routing (CIDR) notation: <i>ip_address/mask</i> (for example, 192.168.2.0/24 for IPv4 or 2001:db8::/32 for IPv6).
Interface	Select the interface to forward packets to the destination, or configure the next hop settings, or both.
Next Hop	Specify the following next hop settings: <ul style="list-style-type: none">• None—Select if there is no next hop for the route.• IP Address—Specify the IP address of the next hop router.• Discard—Select if you want to drop traffic that is addressed to this destination.• Next VR—Select a virtual router in the firewall as the next hop. This option allows you to route internally between virtual routers within a single firewall.
Admin Distance	Specify the administrative distance for the static route (10-240, default 10).
Metric	Specify a valid metric for the static route (1 - 65535).
No Install	Select if you do not want to install the route in the forwarding table. The route is retained in the configuration for future reference.

Configuring the Redistribution Profiles Tab

► *Network > Virtual Router > Redistribution Profiles*

Redistribution Profiles direct the firewall to filter, set priority, and perform actions based on desired network behavior. Route redistribution allows static routes and routes that are acquired by other protocols to be advertised through specified routing protocols. Redistribution profiles must be applied to routing protocols in order to take effect. Without redistribution rules, each protocol runs separately and does not communicate outside its purview. Redistribution profiles can be added or modified after all routing protocols are configured and the resulting network topology is established. Apply redistribution profiles to the RIP and OSPF protocols by defining export rules. Apply redistribution profiles to BGP in the **Redistribution Rules** tab.

Table 88. Virtual Router Settings - Redistribution Profiles Tab

Field	Description
Name	Click Add to display the Redistribution Profile page, and enter the profile name.
Priority	Enter a priority (range 1-255) for this profile. Profiles are matched in order (lowest number first).
Redistribute	<p>Choose whether to perform route redistribution based on the settings in this window.</p> <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 check boxes to specify the route types of the candidate route.
Interface	Select the interfaces to specify the forwarding interfaces of the candidate route.
Destination	To specify the destination of the candidate route, enter the destination IP address or subnet (format x.x.x.x or x.x.x.x/n) and click Add . To remove an entry, click the  icon associated with the entry.
Next Hop	To specify the gateway of the candidate route, enter the IP address or subnet (format x.x.x.x or x.x.x.x/n) that represents the next hop and click Add . To remove an entry, click the  icon associated with the entry.
OSPF Filter Tab	
Path Type	Select check boxes to specify the route types of the candidate OSPF route.
Area	Specify the area identifier for the candidate OSPF route. Enter the OSPF area ID (format x.x.x.x), and click Add . To remove an entry, click the  icon associated with the entry.
Tag	Specify OSPF tag values. Enter a numeric tag value (1-255), and click Add . To remove an entry, click the  icon associated with the entry.
BGP Filter Tab	
Community	Specify a community for BGP routing policy.
Extended Community	Specify an extended community for BGP routing policy.

Configuring the RIP Tab

► *Network > Virtual Router > RIP*

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

Table 89. Virtual Router Settings - RIP Tab

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

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

- **Interfaces** tab: See “[Configuring the Interfaces Tab](#)”.
- **Timers** tab: See “[Configuring the Timers Tab](#)”.
- **Auth Profiles** tab: See “[Configuring the Auth Profiles Tab](#)”.
- **Export Rules** tab: See “[Configuring the Export Rules Tab](#)”.

Configuring the Interfaces Tab

► *Network > Virtual Router > RIP > Interfaces*

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

Table 90. RIP Settings – Interfaces Tab

Field	Description
Interfaces	
Interface	Select the interface that runs the RIP protocol.
Enable	Select to enable these settings.
Advertise	Select to advertise a default route to RIP peers with the specified metric value.
Metric	Specify a metric value for the router advertisement. This field is visible only if the Advertise check box is selected.
Auth Profile	Select the profile.
Mode	Select normal , passive , or send-only .

Configuring the Timers Tab

► *Network > Virtual Router > RIP > Timers*

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

Table 91. RIP Settings – Timers Tab

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

Configuring the Auth Profiles Tab

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

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

Table 92. RIP Settings – Auth Profiles Tab

Field	Description
Auth Profiles	
Profile Name	Enter a name for the authentication profile to authenticate RIP messages. To authenticate RIP messages, first define the authentication profiles and then apply them to interfaces on the RIP tab.
Password Type	Select the type of password (simple or MD5). <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 message, select the Preferred option.

Configuring the Export Rules Tab

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

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

Table 93. RIP Settings – Export Rules Tab

Field	Description
Export Rules	
Export Rules	<p>(Read-only) Displays the rules that apply to routes sent by the virtual router to a receiving router.</p> <ul style="list-style-type: none"> • Allow Redistribute Default Route—Select the check box to permit the firewall to redistribute its default route to peers. • Redistribution Profile—Select a redistribution profile that allows you to modify route redistribution, filter, priority, and action based on the desired network behavior. See “Configuring the Redistribution Profiles Tab”.

Configuring the OSPF Tab

- *Network > Virtual Router > OSPF*

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

Table 94. Virtual Router Settings - OSPF Tab

Field	Description
Enable	Select the check box to enable the OSPF protocol.
Reject Default Route	Select the check box if you do not want to learn any default routes through OSPF. Selecting the check box is recommended, especially for static routes.
Router ID	Specify the router ID associated with the OSPF instance in this virtual router. The OSPF protocol uses the router ID to uniquely identify the OSPF instance.

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

- **Areas** tab: See “[Configuring the Areas Tab](#)”.
- **Auth Profiles** tab: See “[Configuring the Auth Profiles Tab](#)”.
- **Export Rules** tab: See “[Configuring the Export Rules Tab](#)”.
- **Advanced** tab: See “[Configuring the Advanced Tab](#)”.

Configuring the Areas Tab

► *Network > Virtual Router > OSPF > Areas*

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

Table 95. OSPF Settings – Areas Tab

Field	Description
Areas	
Area ID	Configure the area over which the OSPF parameters can be applied. Enter an identifier for the area in x.x.x.x format. This is the identifier that each neighbor must accept to be part of the same area.
Type	Select one of the following options. <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.

Table 95. OSPF Settings – Areas Tab (Continued)

Field	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 the check box to if you do not want the OSPF interface to send or receive OSPF packets. Although OSPF packets are not sent or received if you choose this option, the interface is included in the LSA database. • Link type—Choose Broadcast if you want all neighbors that are accessible through the interface to be discovered automatically by multicasting OSPF hello messages, such as an Ethernet interface. Choose p2p (point-to-point) to automatically discover the neighbor. Choose p2mp (point-to-multipoint) when neighbors must be defined manually. Defining neighbors manually is allowed only for p2mp mode. • Metric—Enter the OSPF metric for this interface (0-65535). • Priority—Enter the OSPF priority for this interface (0-255). It is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) according to the OSPF protocol. When the value is zero, the router will not be elected as a DR or BDR. • Auth Profile—Select a previously-defined authentication profile. • Hello Interval (sec)—Interval at which the OSPF process sends hello packets to its directly connected neighbors. Range: 0-3600 seconds. Default: 10 seconds. • Dead Counts—Number of times the hello interval can occur for a neighbor without OSPF receiving a hello packet from the neighbor, before OSPF considers that neighbor down. The Hello Interval multiplied by the Dead Counts equals the value of the dead timer. Range: 3-20. Default: 4. • Retransmit Interval (sec)—Length of time that OSPF waits to receive a link-state advertisement (LSA) from a neighbor before OSPF retransmits the LSA. Range: 0-3600 seconds. Default: 10 seconds. • Transit Delay (sec)—Length of time that an LSA is delayed before it is sent out of an interface. Range: 0-3600 seconds. Default: 1 second. • Graceful Restart Hello Delay (sec)—Applies to an OSPF interface when Active/Passive High Availability is configured. Graceful Restart Hello Delay is the length of time during which the firewall sends Grace LSA packets at 1-second intervals. During this time, no hello packets are sent from the restarting firewall. During the restart, the dead timer (which is the Hello Interval multiplied by the Dead Counts) is also counting down. If the dead timer is too short, the adjacency will go down during the graceful restart because of the hello delay. Therefore, it is recommended that the dead timer be at least four times the value of the Graceful Restart Hello Delay. For example, a Hello Interval of 10 seconds and a Dead Counts of 4 yield a dead timer of 40 seconds. If the Graceful Restart Hello Delay is set to 10 seconds, that 10-second delay of hello packets is comfortably within the 40-second dead timer, so the adjacency will not time out during a graceful restart. Range: 1-10 seconds. Default: 10 seconds.

Table 95. OSPF Settings – Areas Tab (Continued)

Field	Description
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.

Configuring the Auth Profiles Tab

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

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

Table 96. OSPF Settings – Auth Profiles Tab

Field	Description
Auth Profiles	
Profile Name	Enter a name for the authentication profile. To authenticate the OSPF messages, first define the authentication profiles and then apply them to interfaces on the OSPF tab.
Password Type	<p>Select the type of password (simple or MD5).</p> <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.

Configuring the Export Rules Tab

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

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

Table 97. OSPF Settings – Auth Profiles Tab

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

Table 97. OSPF Settings – Auth Profiles Tab (Continued)

Field	Description
Name	Select the name of a redistribution profile. The value must be an IP subnet or valid redistribution profile name.
New Path Type	Choose the metric type to apply.
New Tag	Specify a tag for the matched route that has a 32-bit value.
Metric	Specify the route metric to be associated with the exported route and used for path selection (optional, range 1-65535).

Configuring the Advanced Tab

► *Network > Virtual Router > OSPF > Advanced*

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

Table 98. OSPF Settings – Advanced Tab

Field	Description
Advanced	
RFC 1583 Compatibility	Select the check box to assure compatibility with RFC 1583.
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: 5 - 1800 seconds. Default: 120 seconds. • Max Neighbor Restart Time – The maximum grace period in seconds that the firewall will accept as a help-mode router. If the peer devices offers a longer grace period in its grace LSA, the firewall will not enter helper mode. Range: 5 - 1800 seconds. Default: 140 seconds.

Configuring the OSPFv3 Tab

► *Network > Virtual Router > OSPFv3*

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

Table 99. Virtual Router Settings - OSPF Tab

Field	Description
Enable	Select the check box to enable the OSPF protocol.
Reject Default Route	Select the check box if you do not want to learn any default routes through OSPF. Selecting the check box is recommended, especially for static routes.
Router ID	Specify the router ID associated with the OSPF instance in this virtual router. The OSPF protocol uses the router ID to uniquely identify the OSPF instance.

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

- **Areas tab:** See “[Configuring the Areas Tab](#)”.
- **Auth Profiles tab:** See “[Configuring the Auth Profiles tab](#)”.
- **Export Rules tab:** See “[Configuring the Export Rules Tab](#)”.
- **Advanced tab:** See “[Configuring the Advanced Tab](#)”.

Configuring the Areas Tab

► *Network > Virtual Router > OSPFv3 > Areas*

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

Table 100. Virtual Router Settings - Areas Tab

Field	Description
Authentication	Select the name of the Authentication profile that you want to specify for this OSPF area.
Type	<p>Select one of the following options.</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	Click Add to aggregate LSA destination IPv6 addresses in the area by subnet. Enable or suppress advertising LSAs that match the subnet, and click OK . Repeat to add additional ranges.

Table 100. Virtual Router Settings - Areas Tab (Continued)

Field	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 the check box to if you do not want the OSPF interface to send or receive OSPF packets. Although OSPF packets are not sent or received if you choose this option, the interface is included in the LSA database. • Link type—Choose Broadcast if you want all neighbors that are accessible through the interface to be discovered automatically by multicasting OSPF hello messages, such as an Ethernet interface. Choose p2p (point-to-point) to automatically discover the neighbor. Choose p2mp (point-to-multipoint) when neighbors must be defined manually. Defining neighbors manually is allowed only for p2mp mode. • Metric—Enter the OSPF metric for this interface (0-65535). • Priority—Enter the OSPF priority for this interface (0-255). It is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) according to the OSPF protocol. When the value is zero, the router will not be elected as a DR or BDR. • Auth Profile—Select a previously-defined authentication profile. • Hello Interval (sec)—Interval at which the OSPF process sends hello packets to its directly connected neighbors. Range: 0-3600 seconds. Default: 10 seconds. • Dead Counts—Number of times the hello interval can occur for a neighbor without OSPF receiving a hello packet from the neighbor, before OSPF considers that neighbor down. The Hello Interval multiplied by the Dead Counts equals the value of the dead timer. Range: 3-20. Default: 4. • Retransmit Interval (sec)—Length of time that OSPF waits to receive a link-state advertisement (LSA) from a neighbor before OSPF retransmits the LSA. Range: 0-3600 seconds. Default: 10 seconds. • Transit Delay (sec)—Length of time that an LSA is delayed before it is sent out of an interface. Range: 0-3600 seconds. Default: 1 second. • Graceful Restart Hello Delay (sec)—Applies to an OSPF interface when Active/Passive High Availability is configured. Graceful Restart Hello Delay is the length of time during which the firewall sends Grace LSA packets at 1-second intervals. During this time, no hello packets are sent from the restarting firewall. During the restart, the dead timer (which is the Hello Interval multiplied by the Dead Counts) is also counting down. If the dead timer is too short, the adjacency will go down during the graceful restart because of the hello delay. Therefore, it is recommended that the dead timer be at least four times the value of the Graceful Restart Hello Delay. For example, a Hello Interval of 10 seconds and a Dead Counts of 4 yield a dead timer of 40 seconds. If the Graceful Restart Hello Delay is set to 10 seconds, that 10-second delay of hello packets is comfortably within the 40-second dead timer, so the adjacency will not time out during a graceful restart. Range: 1-10 seconds. Default: 10 seconds. • Neighbors—For p2mp interfaces, enter the neighbor IP address for all neighbors that are reachable through this interface.

Table 100. Virtual Router Settings - Areas Tab (Continued)

Field	Description
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.

Configuring the Auth Profiles tab

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

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

Table 101. OSPFv3 Settings – Auth Profiles Tab

Field	Description
Auth Profiles	
Profile Name	Enter a name for the authentication profile. To authenticate the OSPF messages, first define the authentication profiles and then apply them to interfaces on the OSPF tab.
SPI	Specify the security parameter index (SPI) for packet traversal from the remote firewall to the peer.
Protocol	Specify either of the following protocols: <ul style="list-style-type: none"> • ESP – Encapsulating Security Payload protocol. • AH – Authentication Header protocol
Crypto Algorithm	Specify one of the following <ul style="list-style-type: none"> • None – No crypto algorithm will be used. • SHA1 – Secure Hash Algorithm 1. • SHA256 – Secure Hash Algorithm 2. A set of four hash functions with a 256 bit digest. • SHA384 – Secure Hash Algorithm 2. A set of four hash functions with a 384 bit digest. • SHA512 – Secure Hash Algorithm 2. A set of four hash functions with a 512 bit digest. • MD5 – The MD5 message-digest algorithm.
Key/Confirm Key	Enter and confirm an authentication key.

Table 101. OSPFv3 Settings – Auth Profiles Tab (Continued)

Field	Description
Encryption	<p>Specify one of the following:</p> <ul style="list-style-type: none"> • aes128 – applies the Advanced Encryption Standard (AES) using cryptographic keys of 128 bits. • aes192 – applies the Advanced Encryption Standard (AES) using cryptographic keys of 192 bits. • aes256 – applies the Advanced Encryption Standard (AES) using cryptographic keys of 256 bits. • null – No encryption is used. <p>Not available if the AH protocol was chosen.</p>
Key/Confirm Key	Enter and confirm an encryption key.

Configuring the Export Rules Tab

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

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

Table 102. OSPF Settings – Auth Profiles Tab

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

Configuring the Advanced Tab

► *Network > Virtual Router > OSPF > Advanced*

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

Table 103. OSPF Settings – Advanced Tab

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

Table 103. OSPF Settings – Advanced Tab (Continued)

Field	Description
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: 5 - 1800 seconds. Default: 120 seconds. Max Neighbor Restart Time – The maximum grace period in seconds that the firewall will accept as a help-mode router. If the peer devices offers a longer grace period in its grace LSA, the firewall will not enter helper mode. Range: 5 - 1800 seconds. Default: 140 seconds.

Configuring the BGP Tab

► *Network > Virtual Router > BGP*

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

Table 104. Virtual Router Settings - BGP Tab

Field	Description
Enable	Select the check box to enable BGP.
Router ID	Enter the IP address to assign to the virtual router.
AS Number	Enter the number of the AS to which the virtual router belongs, based on the router ID (range 1-4294967295).

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

- **General tab:** See “[Configuring the General Tab](#)”.
- **Advanced tab:** See “[Configuring the Advanced Tab](#)”.
- **Peer Group tab:** See “[Configuring the Peer Group Tab](#)”.

- **Import** tab: See “[Configuring the Import and Export Tabs](#)”.
- **Export** tab: See “[Configuring the Import and Export Tabs](#)”.
- **Conditional Adv** tab: See “[Configuring the Conditional Adv Tab](#)”.
- **Aggregate** tab: See “[Configuring the Conditional Adv Tab](#)”.
- **Redist Rules** tab: See “[Configuring the Redist Rules Tab](#)”.

Configuring the General Tab

► *Network > Virtual Router > BGP > General*

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

Table 105. BGP Settings – General Tab

Field	Description
General Tab	
Reject Default Route	Select the check box to ignore any default routes that are advertised by BGP peers.
Install Route	Select the check box to install BGP routes in the global routing table.
Aggregate MED	Select to enable route aggregation even when routes have different Multi-Exit Discriminator (MED) values.
Default Local Preference	Specifies a value than can be used to determine preferences among different paths.
AS Format	Select the 2-byte (default) or 4-byte format. This setting is configurable for interoperability purposes.
Always Compare MED	Enable MED comparison for paths from neighbors in different autonomous systems.
Deterministic MED Comparison	Enable MED comparison to choose between routes that are advertised by IBGP peers (BGP peers in the same autonomous system).
Auth Profiles	<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 the  icon to delete a profile.</p>

Configuring the Advanced Tab

► *Network > Virtual Router > BGP > Advanced*

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

Table 106. BGP Settings – Advanced Tab

Field	Description
Advanced Tab	
Graceful Restart	<p>Activate the graceful restart option.</p> <ul style="list-style-type: none"> • Stale Route Time—Specify the length of time that a route can stay in the stale state (range 1-3600 seconds, default 120 seconds). • Local Restart Time—Specify the length of time that the local device takes to restart. This value is advertised to peers (range 1-3600 seconds, default 120 seconds). • Max Peer Restart Time—Specify the maximum length of time that the local device accepts as a grace period restart time for peer devices (range 1-3600 seconds, default 120 seconds).
Reflector Cluster ID	Specify an IPv4 identifier to represent the reflector cluster.
Confederation Member AS	Specify the identifier for the AS confederation to be presented as a single AS to external BGP peers.
Dampening Profiles	<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 0.0-1000.0, default 1.25). • Reuse—Specify a route withdrawal threshold below which a suppressed route is used again (range 0.0-1000.0, default 5). • Max. Hold Time—Specify the maximum length of time that a route can be suppressed, regardless of how unstable it has been (range 0-3600 seconds, default 900 seconds). • Decay Half Life Reachable—Specify the length of time after which a route's stability metric is halved if the route is considered reachable (range 0-3600 seconds, default 300 seconds). • Decay Half Life Unreachable—Specify the length of time after which a route's stability metric is halved if the route is considered unreachable (range 0-3600 seconds, default 300 seconds).
Click the  icon to delete a profile.	

Configuring the Peer Group Tab

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

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

Table 107. BGP Settings – Peer Group Tab

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

Table 107. BGP Settings – Peer Group Tab (Continued)

Field	Description
Soft Reset with Stored Info	Select the check box to perform a soft reset of the firewall after updating the peer settings.
Type	<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 the following; <ul style="list-style-type: none"> – Export Next Hop • EBGP Confed—Specify the following; <ul style="list-style-type: none"> – Export Next Hop • IBGP Confed—Specify the following; <ul style="list-style-type: none"> – Export Next Hop • EBGP—Specify the following: <ul style="list-style-type: none"> – Import Next Hop – Export Next Hop – Remove Private AS (select if you want to force BGP to remove private AS numbers).
Import Next Hop	<p>Choose an option for next hop import:</p> <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	<p>Choose an option for next hop export:</p> <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.

Table 107. BGP Settings – Peer Group Tab (Continued)

Field	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 0-1200 seconds, default 30 seconds). – Multi Hop—Set the time-to-live (TTL) value in the IP header (range 1-255, default 0). The default value of 0 means 2 for eBGP and 255 for iBGP. – Open Delay Time—Specify the delay time between opening the peer TCP connection and sending the first BGP open message (range 0-240 seconds, default 0 seconds). – Hold Time—Specify the period of time that may elapse between successive KEEPALIVE or UPDATE messages from a peer before the peer connection is closed. (range 3-3600 seconds, default 90 seconds). – Idle Hold Time—Specify the time to wait in the idle state before retrying connection to the peer (range 1-3600 seconds, default 15 seconds). • Peer Address—Specify the IP address and port of the peer. • Advanced Options—Configure the following settings: <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). • Incoming Connections/Outgoing Connections—Specify the incoming and outgoing port numbers and select the Allow check box to allow traffic to or from these ports.

Configuring the Import and Export Tabs

- ▶ *Network > Virtual Router > BGP > Import*
- ▶ *Network > Virtual Router > BGP > Export*

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

Table 108. BGP Settings – Import and Export Tabs

Field	Description
Import Rules/Export Rules Tabs	
Import Rules/Export Rules	<p>Click the BGP Import Rules or Export Rules subtab. To add a new rule, click Add and configure the following settings.</p> <ul style="list-style-type: none"> • General subtab: <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 subtab: <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 subtab: <ul style="list-style-type: none"> – Action—Specify an action (Allow or Deny) to take when the match conditions are met. – Local Preference—Specify a local preference metric, only if the action is Allow. – MED—Specify a MED value, only if the action is Allow (0- 65535). – Weight—Specify a weight value, only if the action is Allow (0- 65535). – Next Hop—Specify a next hop router, only if the action is Allow. – Origin—Specify the path type of the originating route: IGP, EGP, or incomplete, only if the action is Allow. – AS Path Limit—Specify an AS path limit, only if the action is Allow. – AS Path—Specify an AS path: None, Remove, Prepend, Remove and Prepend, only if the action is Allow. – Community—Specify a community option: None, Remove All, Remove Regex, Append, or Overwrite, only if the action is Allow. – Extended Community—Specify a community option: None, Remove All, Remove Regex, Append, or Overwrite, only if the action is Allow. – Dampening—Specify the dampening parameter, only if the action is Allow. <p>Click the  icon to delete a group. Click Clone to add a new group with the same settings as the selected group. A suffix is added to the new group name to distinguish it from the original group.</p>

Configuring the Conditional Adv Tab

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

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

Table 109. BGP Settings – Conditional Adv Tabs

Field	Description
Conditional Adv Tab	The BGP conditional advertisement feature allows you to control what route to advertise in the event that a different route is not available in the local BGP routing table (LocRIB), indicating a peering or reachability failure. This is useful in cases where you want to try and force routes to one AS over another, for example if you have links to the Internet through multiple ISPs and you want traffic to be routed to one provider instead of the other unless there is a loss of connectivity to the preferred provider. With conditional advertising, you can configure a non-exist filter that matches the prefix of the preferred route. If any route matching the non-exist filter is not found in the local BGP routing table, only then will the device allow advertisement of the alternate route (the route to the other, non-preferred provider) as specified in its advertise filter. To configure conditional advertisement, select the Conditional Adv tab and then click Add . The following describes how to configure the values in the fields.
Policy	Specify the policy name for this conditional advertisement rule.
Enable	Select the check box to enable BGP conditional advertisement.
Used By	Click Add and select the peer groups that will use this conditional advertisement policy.
Non Exist Filters Subtab	<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.

Table 109. BGP Settings – Conditional Adv Tabs (Continued)

Field	Description
Advertise Filters Subtab	<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.

Configuring the Aggregate Tab

► *Network > Virtual Router > BGP > Aggregate*

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

Table 110. BGP Settings – Aggregate Tabs

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

Configuring the Redist Rules Tab

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

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

Table 111. BGP Settings – Redist Rules

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

Configuring the Multicast Tab

- *Network > Virtual Router > Multicast*

Configuring Multicast protocols requires configuring the following standard settings:

Table 112. Virtual Router Settings - Multicast Tab

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

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

- **Rendezvous Point** tab: See “[Configuring the Rendezvous Point Tab](#)”.
- **Interfaces** tab: See “[Configuring the Interfaces Tab](#)”.
- **SPT Threshold** tab: See “[Configuring the SPT Threshold Tab](#)”.
- **Source Specific Address Space** tab: See “[Configuring the Source Specific Address Tab](#)”.

Configuring the Rendezvous Point Tab

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

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

Table 113. Multicast Settings – Rendezvous Point Tab

Field	Description
Rendezvous Point Subtab	
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 lists. Select the Override learned RP for the same group check box if you want to use the specified RP instead of the RP elected for this group. • Candidate—Specify the following information for the candidate RP running on this virtual router: <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 the check box to use the specified RP instead of the RP elected for this group. • Group—Specify a list of groups for which the specified address will act as the RP.

Configuring the Interfaces Tab

► *Network > Virtual Router > Multicast > Interfaces*

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

Table 114. Multicast Settings – Interfaces Tab

Field	Description
Interfaces Subtab	
Name	Enter a name to identify an interface group.
Description	Enter an optional description.
Interface	Click Add to specify one or more firewall interfaces.
Group Permissions	<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.

Table 114. Multicast Settings – Interfaces Tab (Continued)

Field	Description
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 the check box to enable the IGMP configuration. • IGMP Version—Choose version 1, 2, or 3 to run on the interface. • Enforce Router-Alert IP Option—Select the check box to require the router-alert IP option when speaking IGMPv2 or IGMPv3. This option must be disabled for compatibility with IGMPv1. • Robustness—Choose an integer value to account for packet loss on a network (range 1-7, default 2). If packet loss is common, choose a higher value. • Max Sources—Specify the maximum number of source-specific memberships allowed on this interface (0 = unlimited). • Max Groups—Specify the maximum number of groups allowed on this interface. • Query Configuration—Specify the following: <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 the check box 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 the check box to allow this interface to receive and/or forward PIM messages • Assert Interval—Specify the interval between PIM assert messages. • Hello Interval—Specify the interval between PIM hello messages. • Join Prune Interval—Specify the interval between PIM join and prune messages (seconds). Default is 60. • DR Priority—Specify the designated router priority for this interface • BSR Border—Select the check box to use the interface as the bootstrap border. • PIM Neighbors—Click Add to specify the list of neighbors that will communicate with using PIM.

Configuring the SPT Threshold Tab

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

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

Table 115. Multicast Settings – SPT Threshold Tab

Field	Description
SPT Threshold Subtab	
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

Configuring the Source Specific Address Tab

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

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

Table 116. Multicast Settings – Source Specific Address Space Tab

Field	Description
Source Specific Address Space Subtab	
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 check box to include the specified groups in the SSM address space.

Defining Security Zones

► *Network > Zones*

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

Table 117. Security Zone Settings

Field	Description
Name	Enter a zone name (up to 15 characters). This name appears in the list of zones when defining security policies and configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.

Table 117. Security Zone Settings (Continued)

Field	Description
Location	This field only appears if the device supports multiple virtual systems (vsys) and that capability is enabled. Select the vsys that applies to this zone.
Type	Select a zone type (Layer2, Layer3, Virtual Wire, Tap, or External virtual system) to list all the interfaces of that type that have not been assigned to a zone. The Layer 2 and Layer 3 zone types list all Ethernet interfaces and subinterfaces of that type. The External virtual system type is for communications among virtual systems in the firewall. Each interface can belong to one zone in one virtual system.
Zone Protection Profiles	Select a profile that specifies how the security gateway responds to attacks from this zone. To add new profiles, see “ Defining Zone Protection Profiles ”.
Log Setting	Select a log forwarding profile for forwarding zone protection logs to an external system. If you have a log forwarding profile that is named <i>default</i> , that profile will be automatically selected for this field when defining a new security zone. You can override this default setting at any time by continuing to select a different log forwarding profile when setting up a new security zone. To define or add a new log forwarding profile (and to name a profile <i>default</i> so that this field is populated automatically), click New (see “ Log Forwarding ”). <i>Note:</i> If you are configuring the zone in a Panorama template, the Log Setting drop-down lists only shared Log Forwarding profiles; to specify a non-shared profile, you must type its name.
Enable User Identification	If you configured User-ID to perform IP address to username mapping (discovery), select this check box to apply the mapping information to traffic in this zone. If you clear the check box, firewall logs, reports, and policies will exclude user mapping information for traffic within the zone. By default, if you select this check box, the firewall applies user mapping information to the traffic of all subnetworks in the zone. To limit the information to specific subnetworks within the zone, use the Include List and Exclude List . Note that User-ID performs discovery for the zone only if it falls within the network range that User-ID monitors. If the zone is outside that range, the firewall does not apply user mapping information to the zone traffic even if you select Enable User Identification . To define the monitored range, see the PAN-OS Administrator's Guide .

Table 117. Security Zone Settings (Continued)

Field	Description
User Identification ACL Include List	By default, if you do not specify subnetworks in this list, the firewall applies the user mapping information it discovers to all the traffic of this zone for use in logs, reports, and policies. To limit the application of user mapping information to specific subnetworks within the zone, then for each subnetwork click Add and select an address (or address group) object or type the IP address range (for example, 10.1.1.1/24). The exclusion of all other subnetworks is implicit: you do not need to add them to the Exclude List. Add entries to the Exclude List only to exclude user mapping information for a subset of the subnetworks in the Include List. For example, if you add 10.0.0.0/8 to the Include List and add 10.2.50.0/22 to the Exclude List , the firewall includes user mapping information for all the zone subnetworks of 10.0.0.0/8 except 10.2.50.0/22, and excludes information for all zone subnetworks outside of 10.0.0.0/8. Note that you can only include subnetworks that fall within the network range that User-ID monitors. To define the monitored range, see the PAN-OS Administrator's Guide .
User Identification ACL Exclude List	To exclude user mapping information for a subset of the subnetworks in the Include List , for each subnetwork to exclude, click Add and select an address (or address group) object or type the IP address range.



If you add entries to the **Exclude List** but not the **Include List**, the firewall excludes user mapping information for all subnetworks within the zone, not just the subnetworks you added.

More Runtime Stats for a Virtual Router

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

- [Routing tab](#): See “[Routing Tab](#)”.
- [RIP tab](#): See “[RIP Tab](#)”.
- [BGP tab](#): See “[BGP Tab](#)”.
- [Multicast tab](#): See “[Multicast Tab](#)”.

Routing Tab

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

Table 118 Routing Runtime Stats

Field	Description
Destination	IPv4 address and netmask or IPv6 address and prefix length of networks the virtual router can reach.
Next Hop	IP address of the device at the next hop toward the Destination network. A next hop of 0.0.0.0 indicates the default route.
Metric	Metric for the route.
Flags	<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. • O1—OSPF external type-1. • O2—OSPF external type-2. • Oi—OSPF intra-area. • Oo—OSPF inter-area.
Age	Age of the route entry in the routing table. Static routes have no age.
Interface	Egress interface of the virtual router that will be used to reach the Next Hop.

RIP Tab

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

Table 119 RIP Runtime Stats

Field	Description
Summary Subtab	
Interval Seconds	Number of seconds in an interval; this value affects the Update, Expire, and Delete Intervals.
Update Intervals	Number of Intervals between RIP route advertisement updates that the virtual router sends to peers.
Expire Intervals	Number of Intervals since the last update the virtual router received from a peer, after which the virtual router marks the routes from the peer as unusable.
Delete Intervals	Number of Intervals after a route has been marked as unusable that, if no update is received, the route is deleted from the routing table.
Interface Subtab	
Address	IP address of an interface on the virtual router where RIP is enabled.
Auth Type	Type of authentication: simple password, MD5, or none.
Send Allowed	Check mark indicates this interface is allowed to send RIP packets.
Receive Allowed	Check mark indicates this interface is allowed to receive RIP packets.

Table 119 RIP Runtime Stats (Continued)

Field	Description
Advertise Default Route	Check mark indicates that RIP will advertise its default route to its peers.
Default Route Metric	Metric (hop count) assigned to the default route. The lower the metric value, the higher priority it has in the route table to be selected as the preferred path.
Key Id	Authentication key used with peers.
Preferred	Preferred key for authentication.
Peer Subtab	
Peer Address	IP address of a peer to the virtual router's RIP interface.
Last Update	Date and time that the last update was received from this peer.
RIP Version	RIP version the peer is running.
Invalid Packets	Count of invalid packets received from this peer. Possible causes that the firewall cannot parse the RIP packet: x bytes over a route boundary, too many routes in packet, bad subnet, illegal address, authentication failed, or not enough memory.
Invalid Routes	Count of invalid routes received from this peer. Possible causes: route is invalid, import fails, or not enough memory.

BGP Tab

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

Table 120 BGP Runtime Stats

Field	Description
Summary Subtab	
Router Id	Router ID assigned to the BGP instance.
Reject Default Route	Indicates whether the Reject Default Route option is configured, which causes the VR to ignore any default routes that are advertised by BGP peers.
Redistribute Default Route	Indicates whether the Allow Redistribute Default Route option is configured.
Install Route	Indicates whether the Install Route option is configured, which causes the VR to install BGP routes in the global routing table.
Graceful Restart	Indicates whether or not Graceful Restart is enabled (support).
AS Size	Indicates whether the AS Format size selected is 2 Byte or 4 Byte.
Local AS	Number of the AS to which the VR belongs.
Local Member AS	Local Member AS number (valid only if the VR is in a confederation). The field is 0 if the VR is not in a confederation.
Cluster ID	Displays the Reflector Cluster ID configured.
Default Local Preference	Displays the Default Local Preference configured for the VR.

Table 120 BGP Runtime Stats (Continued)

Field	Description
Always Compare MED	Indicates whether the Always Compare MED option is configured, which enables a comparison to choose between routes from neighbors in different autonomous systems.
Aggregate Regardless MED	Indicates whether the Aggregate MED option is configured, which enables route aggregation even when routes have different MED values.
Deterministic MED Processing	Indicates whether the Deterministic MED comparison option is configured, which enables a comparison to choose between routes that are advertised by IBGP peers (BGP peers in the same AS).
Current RIB Out Entries	Number of entries in the RIB Out table.
Peak RIB Out Entries	Peak number of Adj-RIB-Out routes that have been allocated at any one time.
Peer Subtab	
Name	Name of the peer.
Group	Name of the peer group to which this peer belongs.
Local IP	IP address of the BGP interface on the VR.
Peer IP	IP address of the peer.
Peer AS	Autonomous system to which the peer belongs.
Password Set	Yes or no indicates whether authentication is set.
Status	Status of the peer, eg. Active, Connect, Established, Idle, OpenConfirm, or OpenSent.
Status Duration (secs.)	Duration of the peer's status.
Peer Group Subtab	
Group Name	Name of a peer group.
Type	Type of peer group configured, such as EBGP or IBGP.
Aggregate Confed. AS	Yes or no indicates whether the Aggregate Confederation AS option is configured.
Soft Reset Support	Yes or no indicates whether the peer group supports soft reset. When routing policies to a BGP peer change, routing table updates might be affected. A soft reset of BGP sessions is preferred over a hard reset because a soft reset allows routing tables to be updated without clearing the BGP sessions.
Next Hop Self	Yes or no indicates whether this option is configured.
Next Hop Third Party	Yes or no indicates whether this option is configured.
Remove Private AS	Indicates whether updates will have private AS numbers removed from the AS_PATH attribute before the update is sent.
Local RIB Subtab	
Prefix	Network prefix and subnet mask in the Local Routing Information Base.
Flag	* indicates the route was chosen as the best BGP route.

Table 120 BGP Runtime Stats (Continued)

Field	Description
Next Hop	IP address of the next hop toward the Prefix.
Peer	Name of peer.
Weight	Weight attribute assigned to the Prefix. If the firewall has more than one route to the same Prefix, the route with the highest weight is installed in the IP routing table.
Local Pref.	Local preference attribute for the route, which is used to choose the exit point toward the prefix if there are multiple exit points. A higher local preference is preferred over a lower local preference.
AS Path	List of autonomous systems in the path to the Prefix network; the list is advertised in BGP updates.
Origin	Origin attribute for the Prefix; how BGP learned of the route.
MED	Multi-Exit Discriminator (MED) attribute of the route. The MED is a metric attribute for a route, which the AS advertising the route suggests to an external AS. A lower MED is preferred over a higher MED.
Flap Count	Number of flaps for the route.
RIB Out Subtab	
Prefix	Network routing entry in the Routing Information Base.
Next Hop	IP address of the next hop toward the Prefix.
Peer	Peer to which the VR will advertise this route.
Local Pref.	Local preference attribute to access the prefix, which is used to choose the exit point toward the prefix if there are multiple exit points. A higher local preference is preferred over a lower local preference.
AS Path	List of autonomous systems in the path to the Prefix network.
Origin	Origin attribute for the Prefix; how BGP learned of the route.
MED	Multi-Exit Discriminator (MED) attribute to the Prefix. The MED is a metric attribute for a route, which the AS advertising the route suggests to an external AS. A lower MED is preferred over a higher MED.
Adv. Status	Advertised status of the route.
Aggr. Status	Indicates whether this route is aggregated with other routes.

Multicast Tab

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

Table 121 Multicast Runtime Stats

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

Table 121 Multicast Runtime Stats (Continued)

Field	Description
IGMP Interface Subtab	
Interface	
Interface	Interface that has IGMP enabled.
Version	Version 1, 2, or 3 of Internet Group Management Protocol (IGMP).
Querier	IP address of the IGMP querier on that interface.
Querier Up Time	Length of time that IGMP querier has been up.
Querier Expiry Time	Time remaining before the current the Other Querier Present timer expires.
Robustness	Robustness variable of the IGMP interface.
Groups Limit	Number of multicast groups allowed on the interface.
Sources Limit	Number of multicast sources allowed on the interface.
Immediate Leave	Yes or no indicates whether Immediate Leave is configured. Immediate leave indicates that the virtual router will remove an interface from the forwarding table entry without sending the interface IGMP group-specific queries.
IGMP Membership Subtab	
Interface	Name of an interface to which the membership belongs.
Group	IP Multicast group address.
Source	Source address of multicast traffic.
Up Time	Length of time this membership been up.
Expiry Time	Length of time remaining before membership expires.
Filter Mode	Include or exclude the source. VR is configured to include all traffic, or only traffic from this source (include), or traffic from any source except this one (exclude).
Exclude Expiry	Time remaining before the interface Exclude state expires.
V1 Host Timer	Time remaining until the local router assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to the interface.
V2 Host Timer	Time remaining until the local router assumes that there are no longer any IGMP Version 2 members on the IP subnet attached to the interface.
PIM Group Mapping Subtab	
Group	IP address of the group mapped to a Rendezvous Point.
RP	IP address of Rendezvous Point for the group.
Origin	Indicates where the VR learned of the RP.
PIM Mode	ASM or SSM.
Inactive	Indicates that the mapping of the group to the RP is inactive.
PIM Interface Subtab	

Table 121 Multicast Runtime Stats (Continued)

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

VLAN Support

► *Network > VLANs*

The firewall supports VLANs that conform to the IEEE 802.1Q standard. Each Layer 2 interface that is defined on the firewall must be associated with a VLAN. The same VLAN can be assigned to multiple Layer 2 interfaces, but each interface can belong to only one VLAN.

Table 122. VLAN Settings

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

DHCP Server and Relay

► *Network > DHCP*

An interface on the firewall can be configured as a DHCP server or DHCP relay agent. A DHCP server on a Layer 3 Ethernet, Aggregated Ethernet, or Layer 3 VLAN interface can assign IP addresses and provide DHCP options to clients. Multiple DHCP servers are supported. Client requests can be forwarded to all servers, with the first server response sent back to the client.

The table lists the fields on the **DHCP Server** and **DHCP Relay** tabs.

Table 123. DHCP Settings

Field	Description
DHCP Server Tab	
Interface	Select the firewall interface to act as a DHCP server.
Mode	Specify that the DHCP server is enabled or disabled , or choose auto mode, which enables the DHCP server, but will disable it if another DHCP server is detected on the network.
Ping IP when allocating new IP	Select the check box to have the DHCP server send a ping message when assigning an IP address to a client. If the ping receives a response, that means a different device already has that address, so it is not available to assign. The DHCP server assigns the next address from the pool.
Lease	Length of time that the DHCP server allocates an IP address to a client. Select Unlimited , or select Timeout and enter the lease duration in Days , Hours , and optionally Minutes . For example, if you enter only hours, then the lease is restricted to that number of hours.
Inheritance Source	Select a source DHCP client interface or PPPoE client interface to propagate various server settings into the DHCP server. If you specify an Inheritance Source , select one or more options that you want inherited from this source. The server can inherit DNS, WINS, NIS, NTP, POP3, and SMTP server addresses, and DNS suffix.
Gateway	Enter the IP address of the network gateway that is used to reach any device not on the same LAN as this DHCP server.
Ippool subnet	Enter the network mask (format <i>x.x.x.x</i>) that applies to the addresses in the IP Pools field.
Primary DNS	Select inherited or enter the IP address of the preferred Domain Name System (DNS) server.
Secondary DNS	Select inherited or enter the IP address of the alternate DNS server.
Primary WINS	Select inherited or enter the IP address of the preferred Windows Internet Naming Service (WINS) server.
Secondary WINS	Select inherited or enter the IP address of the alternate WINS server.
Primary NIS	Select inherited or enter the IP address of the preferred Network Information Service (NIS) server.
Secondary NIS	Select inherited or enter the IP address of the alternate NIS server.
Primary NTP	Select inherited or enter the IP address of the primary Network Time Protocol (NTP) server. If you specify both a primary and secondary NTP server, the firewall will use either without preference.

Table 123. DHCP Settings (Continued)

Field	Description
Secondary NTP	Select inherited or enter the IP address of the secondary NTP server.
POP3 Server	Select inherited or enter the IP address of the Post Office Protocol (POP3) server.
SMTP Server	Select inherited or enter the IP address of the Simple Mail Transfer Protocol (SMTP) server.
DNS Suffix	Select inherited or enter a suffix for the client to use locally when an unqualified hostname is entered that it cannot resolve.
IP Pools	<p>Click Add and specify the range of IP addresses that this server can assign to clients and to which this DHCP configuration applies. You can enter an IP subnet and subnet mask (for example, 192.168.1.0/24) or a range of IP addresses (for example, 192.168.1.10-192.168.1.20).</p> <p>At least one IP pool is required; you can enter multiple IP pools. To edit an existing entry, click Edit, make the changes, and click Done. To delete an entry, click Delete.</p>
Reserved Address	<p>Specify an IP address (format <i>x.x.x.x</i>) from the IP Pools that you do not want the DHCP server to dynamically assign to a client.</p> <p> Optionally enter the MAC Address (format <i>xx:xx:xx:xx:xx:xx</i>) of the device to which you want the Reserved Address permanently assigned. When the client having that MAC Address sends a request to the server, the server will assign the Reserved Address to the client.</p> <p>You can enter multiple reserved addresses and MAC addresses. To edit an existing entry, click Edit, make the changes, and click Done. To delete an entry, click Delete.</p> <p><i>If you leave this area blank, then there will be no reserved IP addresses.</i></p>

DHCP Relay Tab

Interface	Select the firewall interface to act as a DHCP relay agent.
IPv4	Select the IPv4 check box to use IPv4 addresses for DHCP relay and specify IPv4 addresses for up to four DHCP servers.
IPv6	Select the IPv6 check box to use IPv6 addresses for DHCP relay and specify IPv6 addresses for up to four DHCP servers. Specify an outgoing interface if you are using an IPv6 multicast address for your server.

DNS Proxy

► *Network > DNS Proxy*

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

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

Table 124. DNS Proxy Settings

Field	Description
Name	Specify a name to identify the DNS proxy (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Enable	Select the check box to enable 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.
Primary Secondary	Specify the IP addresses of the default primary and secondary DNS servers. If the primary DNS server cannot be found, the secondary will be used.
Check inheritance source	Click the link to see the server settings that are currently assigned to the DHCP client and PPPoE client interfaces. These may include DNS, WINS, NTP, POP3, SMTP, or DNS suffix.
Interface	Select the Interface check box to specify the firewall interfaces to support the DNS proxy rules. Select an interface from the drop-down list and click Add . You can add multiple interfaces. To delete an interface, select the interface and click Delete .
DNS Proxy Rules	Identify DNS proxy server rules. Click Add and specify the following information: <ul style="list-style-type: none"> • Name—A name is required so that a static entry can be reference and modified via the CLI. • Turn on caching of domains resolved by this mapping—Select the check box to enable caching of domains that are resolved by this mapping. • Domain Name—Click Add and enter the proxy server domain name. Repeat to add additional names. To delete a name, select the name and click Delete. For a DNS proxy rule, the number of tokens in a wildcard string must match the number of tokens in the requested domain. For example, “*.engineering.local” will not match “engineering.local”. Both must be specified. • Primary/Secondary—Enter the hostname or IP addresses of the primary and secondary DNS servers.

Table 124. DNS Proxy Settings (Continued)

Field	Description
Static Entries	<p>Provide static FQDN to IP address mappings that will be delivered in response to DNS queries made by hosts. Click Add and specify the following information:</p> <ul style="list-style-type: none"> • Name—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 the IP addresses that map to this domain. <p>Repeat to add additional addresses. To delete an address, select the address and click Delete.</p>
Advanced	<p>Specify the following information:</p> <ul style="list-style-type: none"> • Cache—Select the check box to enable DNS caching and specify the following information: <ul style="list-style-type: none"> – Size—Specify the number of entries that the cache will hold (range 1024-10240, default 1024). – Timeout—Specify the length of time (hours) after which all cached entries are removed. DNS time-to-live values are used to remove cache entries when they have been stored for less than the configured timeout period. Following a timeout, new requests must be resolved and cached again (range 4 to 24, default 4 hours). • TCP Queries—Select the check box to enable DNS queries using TCP and specify the following information: <ul style="list-style-type: none"> – Max Pending Requests—Specify the upper limit on the number of concurrent pending TCP DNS requests that the firewall will support (range 64-256, default 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 1-30, default 2 seconds). – Attempts—Specify the maximum number of attempts (excluding the first attempt) after which the next DNS server is tried (range 1-30, default 5).

Defining Interface Management Profiles

► *Network > Network Profiles > Interface Mgmt*

Use this page to specify the protocols that are used to manage the firewall. To assign management profiles to each interface, see “[Configuring a Layer 3 Ethernet Interface](#)” and “[Configuring a Layer 3 Ethernet Subinterface](#)”.

Table 125. Interface Management Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of interface management profiles when configuring interfaces. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Ping	Select the check box for each service you want to enable on the interfaces to which you assign the profile.
Telnet	
SSH	
HTTP	If you select the Response Pages check box, the ports used to serve Captive Portal response pages are left open on Layer 3 interfaces: port 6080 for NTLM, 6081 for Captive Portal in transparent mode, and 6082 for Captive Portal in redirect mode.
HTTP OCSP	
HTTPS	Selecting the User-ID check box enables communication between firewalls when one redistributes user mapping and group mapping information to the others. For details, see “ User-ID Agents Tab ”.
SNMP	
Response Pages	
User-ID	
User-ID Syslog Listener-	
SSL	
User-ID Syslog Listener-	
UDP	
Permitted IP Addresses	Enter the list of IPv4 or IPv6 addresses from which firewall management is allowed.

Defining Monitor Profiles

► *Network > Network Profiles > Monitor*

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

Table 126. Monitor Settings

Field	Description
Name	Enter a name to identify the monitor profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Action	<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 2-10, default 3).
Threshold	Specify the number of heartbeats to be lost before the firewall takes the specified action (range 2-10, default 5).

Defining Zone Protection Profiles

► *Network > Network Profiles > Zone Protection*

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

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

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

Table 127. Zone Protection Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of zone protection profiles when configuring zones. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, and underscores.
Description	Enter an optional description for the zone protection profile.

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

- **Flood Protection** tab: See “[Configuring Flood Protection](#)”.
- **Reconnaissance Profile** tab: See “[Configuring Reconnaissance Protection](#)”.

- **Packet Based Attack Protection** tab: See “[Configuring Packet Based Attack Protection](#)”.



If you have a multi virtual system environment, and have enabled the following:

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

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

- SYN cookies
- IP fragmentation
- ICMPv6

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

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

Configuring Flood Protection

- *Network > Network Profiles > Zone Protection > Flood Protection*

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

Table 128. Flood Protection tab Settings

Field	Description
Flood Protection Thresholds - SYN Flood	
Action	Select the action to take in response to a SYN flood attack. <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. Alarms can be viewed on the Dashboard (see “ Using the Dashboard ”) and in the threat log (see “ Taking Packet Captures ”).
Activate (packets/sec)	Enter the number of SYN packets received by the zone (in a second) that triggers the action specified.
Maximum (packets/sec)	Enter the maximum number of SYN packets able to be received per second. Any number of packets exceeding the maximum will be dropped.

Table 128. Flood Protection tab Settings (Continued)

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

Configuring Reconnaissance Protection

- *Network > Network Profiles > Zone Protection > Reconnaissance Protection*

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

Table 129. Reconnaissance Protection tab Settings

Field	Description
Reconnaissance Protection - TCP Port Scan, UDP Port Scan, Host Sweep	
Interval (sec)	Enter the time interval for port scans and host sweep detection (seconds).
Threshold (events)	Enter the number of scanned ports within the specified time interval that will trigger this protection type (events).
Action	<p>Enter the action that the system will take in response to this event type:</p> <ul style="list-style-type: none"> • Allow—Permits the port scan or host sweep reconnaissance. • Alert—Generates an alert for each scan or sweep that matches the threshold within the specified time interval. • Block—Drops all further packets from the source to the destination for the remainder of the specified time interval. • Block IP—Drops all further packets for a specified period of time. Choose whether to block source, destination, or source-and-destination traffic and enter a duration (seconds).
IPv6 Drop Packets with	
Type 0 Router Header	Select the check box to drop IPv6 packets that include a Type 0 router header.
IPv4 Compatible Address	Select the check box to drop IPv6 packets that include an IPv4-compatible address.
Multicast Source Address	Select the check box to drop IPv6 packets that include a multicast source address.
Anycast Source Address	Select the check box to drop IPv6 packets that include an anycast source address.

Configuring Packet Based Attack Protection

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

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

- **TCP/IP Drop:** See “[Configuring the TCP/IP Drop tab](#)”.
- **ICMP Drop:** See “[Configuring the ICMP Drop Tab](#)”.
- **IPv6 Drop:** See “[Configuring the IPv6 Drop Tab](#)”.
- **ICMPv6:** See “[Configuring the ICMPv6 Drop tab](#)”.

Configuring the TCP/IP Drop tab

To configure TCP/IP Drop, specify the following settings:

Table 130. IP Drop and TCP Drop tab Settings

Field	Description
TCP/IP Drop sub tab	
Spoofed IP address	Select the check box to enable protection against IP address spoofing.

Table 130. IP Drop and TCP Drop tab Settings (Continued)

Field	Description
Fragmented traffic	Discards fragmented IP packets.
Mismatched overlapping TCP segment	This setting will cause the firewall to report an overlap mismatch and drop the packet when segment data does not match in these scenarios: <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.
	This protection mechanism uses sequence numbers to determine where packets reside within the TCP data stream.
Remove TCP Timestamp	Determines whether the packet has a TCP timestamp in the header and, if it does, strips the timestamp from the header.
Reject Non-SYN TCP	Determines whether to reject the packet, if the first packet for the TCP session setup is not a SYN packet: <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	Determine whether to drop or bypass packets that contain out of sync ACKs or out of window sequence numbers: <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.
IP Option Drop	
Strict Source Routing	Discard packets with the Strict Source Routing IP option set.
Loose Source Routing	Discard packets with the Loose Source Routing IP option set.
Timestamp	Discard packets with the Timestamp IP option set.
Record Route	Discard packets with the Record Route IP option set.
Security	Discard packets if the security option is defined.
Stream ID	Discard packets if the Stream ID option is defined.
Unknown	Discard packets if the class and number are unknown.
Malformed	Discard packets if they have incorrect combinations of class, number, and length based on RFC 791, 1108, 1393, and 2113.

Configuring the ICMP Drop Tab

To configure ICMP Drop, specify the following settings:

Table 131. ICMP Drop tab Settings

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

Table 131. ICMP Drop tab Settings (Continued)

Field	Description
ICMP Large Packet (>1024)	Discards ICMP packets that are larger than 1024 bytes.
Suppress ICMP TTL Expired Error	Stops sending ICMP TTL expired messages.
Suppress ICMP Frag Needed	Stops sending ICMP fragmentation needed messages in response to packets that exceed the interface MTU and have the do not fragment (DF) bit set. This setting will interfere with the PMTUD process performed by hosts behind the firewall.

Configuring the IPv6 Drop Tab

To configure IPv6 Drop, specify the following settings:

Table 132. IPv6 Drop tab Settings

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

Configuring the ICMPv6 Drop tab

To configure ICMPv6 Drop, specify the following settings:

Table 133. ICMPv6 Drop tab Settings

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

Chapter 5

Policies and Security Profiles

This section describes how to configure policies and security profiles:

- [“Policy Types”](#)
- [“Guidelines on Defining Policies”](#)
- [“Security Profiles”](#)
- [“Other Policy Objects”](#)

Policy Types

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

- Basic security policies to block or allow a network session based on the application, the source and destination zones and addresses, and optionally the service (port and protocol). Zones identify the physical or logical interfaces that send or receive the traffic. See [“Defining Security Policies”](#).
- Network Address Translation (NAT) policies to translate addresses and ports, as needed. See [“Defining Network Address Translation Policies”](#).
- Policy-based forwarding policies to determine the egress interface used following processing. See [“Policy-Based Forwarding Policies”](#).
- Decryption policies to specify traffic decryption for security policies. Each policy can specify the categories of URLs for the traffic you want to decrypt. SSH decryption is used to identify and control SSH tunneling in addition to SSH shell access. See [“Decryption Policies”](#).
- Override policies to override the application definitions provided by the firewall. See [“Defining Application Override Policies”](#).
- Quality of Service (QoS) policies to determine how traffic is classified for treatment when it passes through an interface with QoS enabled. See [“Defining QoS Policies”](#).

- Captive portal policies to request authentication of unidentified users. See “[Defining Captive Portal Policies](#)”.
- Denial of service (DoS) policies to protect against DoS attacks and take protective action in response to rule matches. See “[Defining DoS Policies](#)”.

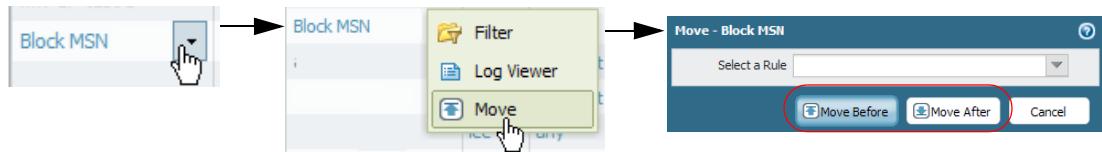


Shared policies pushed from Panorama are shown in green on the firewall web interface pages and cannot be edited at the device level.

Guidelines on Defining Policies

The following specific guidelines apply when interacting with the pages on the **Policies** tab:

- The default rules that instruct the firewall on how to handle traffic that does not match any other rule in the rulebase are displayed at the bottom of the Security rulebase. These rules are predefined on the firewall to allow all intrazone traffic and deny all interzone traffic. 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.
- To apply a filter to the list, select from the **Filter Rules** drop-down list. To add a value to define a filter, click the down-facing arrow for the item and choose **Filter**. Note that the default rules are not part of the rulebase filtering and always show up in the list of filtered rules.
- To view application groups, filters, or container information when creating or viewing Security, PBF, or QoS policies, hold your mouse over the object in the **Application** column, click the down arrow and select **Value**. This allows you to easily view application members directly from the policy without having to navigate to the Object tabs.
- To add a new policy rule, do one of the following:
 - Click **Add** at the bottom of the page.
 - Select a rule on which to base the new rule and click **Clone Rule**, or select a rule by clicking the white space of the rule, and select **Clone Rule** at the bottom of the page (a selected rule has 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.
- The order in which rules are listed is the order in which the rules are compared against network traffic. Change the ordering of a rule in either of the following ways:
 - Select the rule and click **Move Up**, **Move Down**, **Move Top**, or **Move Bottom**.
 - Click the down-facing arrow for the rule name and choose **Move**. In the pop-up window, choose a rule and choose whether to move the rule you selected for reordering before or after this rule.



- To enable a rule, select the rule and click **Enable**.
- To show which rules are not currently used, select the **Highlight Unused Rules** check box.

Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Do Not Log Traffic filter	No Log	tapzone	any	any	any	tapzone	LocalServers	any	any	✓
Do Not Log URL	No Log	tapzone	any	any	any	tapzone	LocalNetwork	ssl	web-browsing	✓

Rule used

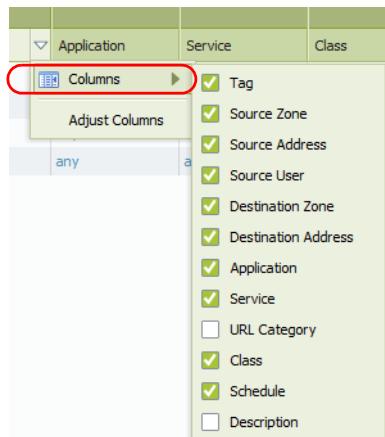
Rule not used (yellow dotted background)

- To display the log for the policy, click the down-facing arrow for the rule name and choose **Log Viewer**.
- For some entries, you can display the current value by clicking the down-facing arrow for the entry and choosing **Value**. You can also edit, filter, or remove certain items directly from the column menu.

- If you have a large number of policies defined, you can use the filter bar to find objects that are used within a policy based on the object name or IP address. The search will also traverse embedded objects to find an address within an address object or address group. In the following screen shot, the IP address 10.8.10.177 was entered in the filter bar and the policy "aaa" is shown. That policy uses an address group object named "aaagroup", which contains the IP address.

Name	Tag	Zone	Address	User	HIP Profile	Zone
1 aaa	none	any	aaagroup bbbgroup	any	any	any

- You can show or hide specific columns from view in any of the **Policies** pages.



Specifying Users and Applications for Policies

- ▶ *Policies > Security*
- ▶ *Policies > Decryption*

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

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

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



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

2. Click the drop-down menu above the **Source User** table to select the user type:
 - **any**—Include any traffic regardless of user data.
 - **pre-logon**—Include remote users that are connected to the network using GlobalProtect, but are not logged into their system. When the Pre-logon option is configured on the Portal for GlobalProtect clients, any user who is not currently logged into their machine will be identified with the username **pre-logon**. You can then create policies for pre-logon users and although the user is not logged in directly, their machines are authenticated on the domain as if they were fully logged in.
 - **known-user**—Includes all authenticated users, which means any IP with user data mapped. This option is equivalent to the “domain users” group on a domain.
 - **unknown**—Includes all unauthenticated users, which means IP addresses that are not mapped to a user. For example, you could use unknown for guest level access to something because they will have an IP on your network, but will not be authenticated to the domain and will not have IP to user mapping information on the firewall.
 - **Select**—Includes selected users as determined by the selection in this window. For example, you may want to add one user, a list of individuals, some groups, or manually add users.

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

Defining Policies on Panorama

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

Pre rules and Post rules can be defined in a shared context as shared policies for all managed devices, or in a device group context to make it specific to a device group. Because Pre rules and Post Rules are defined on Panorama and then pushed from Panorama to the managed devices, you can view the rules on the managed firewalls, but can only edit the Pre Rules and Post Rules in Panorama.

- **Pre Rules**—Rules that are added to the top of the rule order and are evaluated first. You can use pre-rules to enforce the Acceptable Use Policy for an organization; for example, to block access to specific URL categories, or to allow DNS traffic for all users.
- **Post Rules**—Rules that are added at the bottom of the rule order and are evaluated after the pre-rules and the rules locally defined on the device. Post-rules typically include rules to deny access to traffic based on the App-ID, User-ID, or Service.
- **Default Rules**—Rules that instruct the firewall how to handle traffic that does not match any Pre Rules, Post Rules, or local device rules. These rules are part of Panorama's predefined configuration. You must **Override** them to enable editing of select settings in these rules.

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

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

- [“Defining Security Policies”](#)
- [“Defining Network Address Translation Policies”](#)
- [“Defining QoS Policies”](#)
- [“Policy-Based Forwarding Policies”](#)
- [“Decryption Policies”](#)
- [“Defining Application Override Policies”](#)
- [“Defining Captive Portal Policies”](#)
- [“Defining DoS Policies”](#)

Defining Security Policies

► *Policies > Security*

Use this page to define security policies that will determine whether to block or allow a new network session based on traffic attributes such as the application, source and destination security zones, the source and destination addresses, the application service (such as HTTP) and/or user/group.

Security policies 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 defined rules, the default rules apply. The default rules—displayed at the bottom of the security rulebase—are predefined to allow all intrazone (within the zone) traffic and deny all interzone (between zones) traffic. 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. On Panorama, you can also override the default rules and then push them to managed firewalls as part of a device group or shared context. In this case, you can still override these default rules on the firewall, similarly to how you can override settings pushed from a template. If you want to go back to the predefined settings or the settings pushed from Panorama, you can **Revert** the default rules.

For configuration guidelines and information on other policy types, see “[Policies and Security Profiles](#)”. For information on defining policies on Panorama, see “[Defining Policies on Panorama](#)”.

Click **Add** to define a new rule, click **Clone** to copy an existing rule, or click on a rule **Name** to edit an existing rule. The following tables describe the fields for adding or editing a security rule:

- “[General Tab](#)”
- “[Source Tab](#)”
- “[User Tab](#)”
- “[Destination Tab](#)”
- “[Application Tab](#)”
- “[Service/URL Category Tab](#)”
- “[Actions Tab](#)”

General Tab

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

Table 134. Security Policy Settings (General Tab)

Field	Description
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. Only the name is required.

Table 134. Security Policy Settings (General Tab) (Continued)

Field	Description
Rule Type	<p>Specifies whether the rule applies to traffic within a zone, between zones, or both:</p> <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 role with source zones A and B and destination zones A and B, the rule would apply to all traffic within zone A, all traffic within zone B, and all traffic from zone A to zone B and all traffic from zone B to zone A. • intrazone—Applies the rule to all matching traffic within the specified source zones (you cannot specify a destination zone for intrazone rules). For example, if you set the source zone to A and B, the rule would apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B. • interzone—Applies the rule to all matching traffic between the specified source and destination zones. For example, if you set the source zone to A, B, and C and the destination zone to A and B, the rule would apply to traffic from zone A to zone B, from zone B to zone A, from zone C to zone A, and from zone C to zone B, but not traffic within zones A, B, or C.
Description	Enter a description for the policy (up to 255 characters).
Tag	<p>If you need to tag the policy, click Add to specify the tag.</p> <p>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.</p> <p>You can also add tags to the default rules.</p>

Source Tab

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

Table 135. Security Policy Settings (Source Tab)

Field	Description
Source Zone	<p>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, see “Defining Security 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>
Source Address	Click Add to add source addresses, address groups, or regions (default is any). Select from the drop-down list, or click the Address , Address Group , or Regions link at the bottom of the drop-down list, and specify the settings.

User Tab

Use the **User** tab to have the policy perform the defined actions based on an individual user or 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 by a host information profile (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.

Table 136. Security Policy Settings (User Tab)

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. <p><i>Note: If you are using a RADIUS server and not the User-ID Agent, the list of users is not displayed, and you must enter user information manually.</i></p>
HIP Profiles	Click Add to choose Host Information Profiles (HIP) to identify users.

Destination Tab

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

Table 137. Security Policy Settings (Destination Tab)

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, see “Defining Security 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><i>Note: On intrazone rules, you cannot define a Destination Zone because these types of rules only match traffic with a source and a destination within the same zone. To specify the zones that match an intrazone rule you only need to set the Source Zone.</i></p>
Destination Address	<p>Click Add to add destination addresses, address groups, or regions (default is any). Select from the drop-down list, or click the Address link at the bottom of the drop-down list, and specify address settings.</p>

Application Tab

Use the **Application** tab to have the policy action occur based on an application or application group. An administrator can also use an existing App-ID signature and customize it to detect proprietary applications or to detect specific attributes of an existing application. Custom applications are defined in **Objects > Applications**.

Table 138. Security Policy Settings (Application Tab)

Field	Description
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 container in the security 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 allows you to easily view application members directly from the policy without having to navigate to the Object tabs.</p>

Service/URL Category Tab

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

Table 139. Security Policy Settings (Service/URL Category Tab)

Field	Description
Service	Select services to limit to specific TCP and/or UDP port numbers. Choose one of the following from the drop-down list: <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 protocols, which if not intentional, can be a sign of undesired application behavior and usage. Note that when you use this option, the device still checks for all applications on all ports, but with this configuration, applications are only allowed on their default ports/protocols. • Select—Click Add. Choose an existing service or choose Service or Service Group to specify a new entry. See “Services” and “Service Groups”.
URL Category	Select URL categories for the security rule. <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 list. You can add multiple categories. See “Dynamic Block Lists” for information on defining custom categories.

Actions Tab

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

Table 140. Security Policy Settings (Actions Tab)

Field	Description
Action Setting	<p>Click allow or deny to allow or block a new network session for traffic that matches this rule.</p> <p>You can also change the Action settings on the default rules.</p>
Profile Setting	<p>Associate profiles or profile groups with the security rule:</p> <ul style="list-style-type: none"> • To specify the checking done by the default security profiles, select individual Antivirus, Anti-spyware, Vulnerability Protection, URL Filtering, File Blocking, and/or Data Filtering profiles. • To specify a profile group, rather than individual profiles, select Profile Type Group and then select a profile group from the Group Profile drop-down list. If you have a security profile group configured that is named <i>default</i>, the Profile Settings will be automatically populated to use that default security profile group: the Profile Type will be set to Group and the Group Profile field will show the <i>default</i> security profile group selected by default. Go to Objects > Security Profile Groups to add a security profile group and name the group <i>default</i>, in order for new security policies to automatically be associated with the <i>default</i> security profile group. You can override this default setting at any time by continuing to modify the Profile Setting fields as you choose. • To define new profiles or profile groups, click New next to the appropriate profile or group (see “Security Profile Groups”).

Table 140. Security Policy Settings (Actions Tab)

Field	Description
Log Setting	<p>Specify any combination of the following options:</p> <ul style="list-style-type: none"> • 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 (disabled by default). – Log At Session End. Generates a traffic log entry for the end of a session (enabled by default). • If the session start or end entries are logged, drop and deny entries are also logged. • Log Forwarding Profile—To forward the local traffic log and threat log entries to remote destinations, such as Panorama and syslog servers, select a log profile from the Log Forwarding Profile drop-down list. Note that the generation of threat log entries is determined by the security profiles. If you have a log forwarding profile that is named <i>default</i>, that profile will be automatically selected for this field when creating new security policies. You can override this default setting at any time by continuing to select a different log forwarding profile when setting up a new security policy. To define or add a new log forwarding profile (and to name a profile <i>default</i> so that this field is populated automatically), click New (see “Log Forwarding”). <p>You can also modify the log settings on the default rules.</p>
Other Settings	<p>Specify any combination of the following options:</p> <ul style="list-style-type: none"> • Schedule—To limit the days and times when the rule is in effect, select a schedule from the drop-down list. To define new schedules, click New (see “Schedules”). • 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 list. For more information on QoS, see “Configuring Quality of Service”. • Disable Server Response Inspection—To disable packet inspection from the server to the client, select this check box. This option may be useful under heavy server load conditions.

NAT Policies

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

NAT is also supported on virtual wire interfaces. When performing NAT on virtual wire interfaces, it is recommended that you translate the source address to a different subnet than the one on which the neighboring devices are communicating. Proxy ARP is not supported on virtual wires and so neighboring devices will only be able to resolve ARP requests for IP addresses that reside on the interface of the device on the other end of the virtual wire.

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

The firewall supports the following types of address translation:

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



Palo Alto Networks Dynamic IP/port NAT supports more NAT sessions than are supported by the number of available IP addresses and ports. The firewall can use IP address and port combinations up to two times (simultaneously) on the PA-200, PA-500, PA-2000 Series and PA-3000 Series, four times on the PA-4020 and PA-5020, and eight times on the PA-4050, PA-4060, PA-5050, PA-5060, and PA-7050 devices when destination IP addresses are unique.

- **Dynamic IP**—For outbound traffic. Private source addresses translate to the next available address in the specified address range. Dynamic IP NAT policies allow you to specify a single IP address, multiple IPs, multiple IP ranges, or multiple subnets as the translated address pool. If the source address pool is larger than the translated address pool, new IP addresses seeking translation will be blocked while the translated address pool is fully utilized. To avoid this issue, you can specify a fall back pool that will be used if the primary pool runs out of IP addresses.
- **Static IP**—For inbound or outbound traffic. You can use static IP to change the source or the destination IP address while leaving the source or destination port unchanged. When used to map a single public IP address to multiple private servers and services, destination ports can stay the same or be directed to different destination ports.



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

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

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

Table 141. NAT Types

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

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

Determining Zone Configuration in NAT and Security Policy

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

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

NAT Rule Options

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

No-NAT Rules

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

Bi-directional NAT Rules

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

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

Figure 2. Bi-Directional NAT Rules

NAT Policy Examples

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

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

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

Figure 3. Dynamic Source Address Translation

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

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

Figure 4. Static Source and Destination Address Translation

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

NAT64

[NAT64](#) provides a way to transition to IPv6 while you still need to communicate with IPv4 networks. When you need to communicate from an IPv6-only network to an IPv4 network, you use NAT64 to translate source and destination addresses from IPv6 to IPv4 and vice versa. NAT64 allows IPv6 clients to access IPv4 servers and allows IPv4 clients to access IPv6 servers. You should understand “[NAT Policies](#)” before configuring NAT64.

If you want to perform NAT64 translation using IPv6-Initiated Communication, you must use a third-party [DNS64 server](#) or other DNS64 solution that is set up with the Well-Known Prefix or your NSP.

You can [configure NAT64](#) for two types of translation on the firewall; each one is doing a bi-directional translation between the two IP address families. Depending on whether the initial translation is from IPv6 to IPv4, or IPv4 to IPv6, configure IPv6-initiated communication or IPv4-initiated communication, respectively. IPv4-initiated communication offers an additional option to translate port numbers.

Defining Network Address Translation Policies

► [Policies > NAT](#)

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

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

For configuration guidelines and information on other policy types, see “[Policies and Security Profiles](#)”.

For information on defining policies on Panorama, see “[Defining Policies on Panorama](#)”.

The following tables describe the NAT settings:

- [“General Tab”](#)
- [“Original Packet Tab”](#)
- [“Translated Packet Tab”](#)

General Tab

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

Table 142. NAT Rule Settings (General Tab)

Field	Description
Name	Change the default rule name and/or enter a rule description.
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.
NAT Type	Specify ipv4 for NAT between IPv4 addresses, or nat64 translation between IPv6 and IPv4 addresses. <i>You cannot combine IPv4 and IPv6 address ranges in a single NAT rule.</i>

Original Packet Tab

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

Table 143. NAT Rule Settings (Original Packet Tab)

Field	Description
Source Zone Destination Zone	Select one or more source and destination zones for the original (non-NAT) packet (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, see "Defining Security Zones" . Multiple zones can be used to simplify management. For example, you can configure settings so that multiple internal NAT addresses are directed to the same external IP address.
Destination Interface	Specify the type of interface for translation. The destination interface can be used to translate IP addresses differently in the case where the network is connected to two ISPs with different IP address pools.
Service	Specify the services for which the source or destination address is translated. To define new service groups, see "Service Groups" .
Source Address Destination Address	Specify a combination of source and destination addresses for which the source or destination address must be translated.

Translated Packet Tab

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

Table 144. NAT Rule Settings (Translated Packet Tab)

Field	Description
Source Address Translation	<p>Enter an IP address or address range (address1-address2) that the source address is translated to, and select a dynamic or static address pool. 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, four times on the PA-4020 and PA-5020, and eight times on the PA-4050, PA-4060, PA-5050, and PA-5060 devices 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. <ul style="list-style-type: none"> – Advanced (Fall back Dynamic IP Translation)—Use this option to create a fall back pool that will perform IP and port translation and will be used if the primary pool runs out of addresses. You can define addresses for the pool by using the Translated Address option or the Interface Address option, which is for interfaces that receive an IP address dynamically. When creating a fall back pool, make sure addresses do not overlap with addresses in the primary pool. • Static IP—The same address is always used, 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. • None—Translation is not performed.
Destination Address Translation	Enter an IP address or range of IP addresses and a translated port number (1 to 65535) that the destination address and port number are translated to. If the Translated Port field is blank, the destination port is not changed. Destination translation is typically used to allow an internal server, such as an email server, to be accessed from the public network.

Policy-Based Forwarding Policies

► *Policies > Policy Based Forwarding*

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

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

For configuration guidelines and information on other policy types, see “[Policies and Security Profiles](#)”.

For information on defining policies on Panorama, see “[Defining Policies on Panorama](#)”.

The following tables describe the policy-based forwarding settings:

- “[General Tab](#)”
- “[Source Tab](#)”
- “[Destination/Application/Service Tab](#)”
- “[Forwarding Tab](#)”

General Tab

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

Field	Description
Name	Enter a name to identify the rule (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.
Description	Enter a description for the policy (up to 255 characters).
Tag	If you need to tag the policy, click Add to specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.

Source Tab

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

Field	Description
Source Zone	<p>To choose source zones (default is any), click Add and select from the drop-down list. To define new zones, see “Defining Security 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>Note: 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 list, or click the Address, Address Group, or Regions link at the bottom of the drop-down list, 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 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>Note: If you are using a RADIUS server and not the User-ID Agent, the list of users is not displayed, and you must enter user information manually.</p>

Destination/Application/Service Tab

Use the **Destination/Application/Service** tab to define the destination settings that will 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). Select from the drop-down list, or click the Address , Address Group , or Regions link at the bottom of the drop-down list, and specify the settings.
Application	Select specific applications for the PBF rule. To define new applications, see “ Defining Applications ”. To define application groups, see “ Defining Application Groups ”.

Forwarding Tab

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

Field	Description
Action	Select one of the following options: <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 list. • Discard—Drop the packet. • No PBF—Do not alter the path that the packet will take. This option, excludes the packets that match the criteria for source/destination/application/service defined in the rule. Matching packets use the route table instead of PBF; the firewall uses the route table to exclude the matched traffic from the redirected port.
Egress Interface	Directs the packet to a specific Egress Interface
Next Hop	If you direct the packet to a specific interface, specify the Next Hop IP address for the packet.
Monitor	Enable Monitoring to verify connectivity to a target IP Address or to the Next Hop IP address. Select Monitor and attach a monitoring Profile (default or custom) that specifies the action when the IP address is unreachable.
Enforce Symmetric Return	(Required for asymmetric routing environments) Select Enforce Symmetric Return and enter one or more IP addresses in the Next Hop Address List . Enabling symmetric return ensures that return traffic (say, from the Trust zone on the LAN to the Internet) is forwarded out through the same interface through which traffic ingresses from the Internet.

Field	Description
Schedule	To limit the days and times when the rule is in effect, select a schedule from the drop-down list. To define new schedules, see " Schedules ".

Decryption Policies

► *Policies > Decryption*

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

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

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

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

For configuration guidelines and information on other policy types, see "[Policies and Security Profiles](#)".

For information on defining policies on Panorama, see "[Defining Policies on Panorama](#)".



Certain applications will not function if they are decrypted by the firewall. To prevent this from occurring, PAN-OS will not decrypt the SSL traffic for these applications and the decryption rule settings will not apply.

The following tables describe the decryption policy settings:

- ["General Tab"](#)
- ["Source Tab"](#)
- ["Destination Tab"](#)
- ["URL Category Tab"](#)
- ["Options Tab"](#)

General Tab

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

Field	Description
Name	Enter a name to identify the rule (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.
Description	Enter a description for the rule (up to 255 characters).
Tag	If you need to tag the policy, click Add to specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.

Source Tab

Use the **Source** tab to define the source zone or source address that defines the incoming source traffic to which the 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, see "Defining Security Zones" . Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.
Source Address	Click Add to add source addresses, address groups, or regions (default is any). Select from the drop-down list, or click the Address, Address Group, or Regions link at the bottom of the drop-down list, and specify the settings. Select the Negate check box to choose any address except the configured ones.

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. <p><i>Note: If you are using a RADIUS server and not the User-ID Agent, the list of users is not displayed, and you must enter user information manually.</i></p>

Destination Tab

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

Field	Description
Destination Zone	<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, see “Defining Security 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 list, or click the Address, Address Group, or Regions link at the bottom of the drop-down list, and specify the settings. Select the Negate check box to choose any address except the configured ones.</p>

URL Category Tab

Use the **URL Category** tab to apply the decryption policy to any URL category, or specify a list of URL categories to which the policy will be applied.

Field	Description
URL Category Tab	Select URL categories for the decryption rule. <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 list. You can add multiple categories. See “Dynamic Block Lists” for information on defining custom categories.

Options Tab

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

Field	Description
Action	Select decrypt or no-decrypt for the traffic.
Type	Select the type of traffic to decrypt from the drop-down list: <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	Select an existing decryption profile, or create a new decryption profile. See “ Decryption Profiles ”.

Defining Application Override Policies

► *Policies > Application Override*

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

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

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

To create a custom application with application override:

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

For configuration guidelines and information on other policy types, see “[Policies and Security Profiles](#)”.

For information on defining policies on Panorama, see “[Defining Policies on Panorama](#)”.

Use the following tables to configure an application override rule.

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

General Tab

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

Field	Description
Name	Enter a name to identify the rule (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.
Description	Enter a description for the rule (up to 255 characters).
Tag	If you need to tag the policy, click Add to specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.

Source Tab

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

Field	Description
Source Zone	Click Add to choose source zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire). To define new zones, see “ Defining Security Zones ”. Multiple zones can be used to simplify management. For example, if you have three different internal zones (Marketing, Sales, and Public Relations) that are all directed to the untrusted destination zone, you can create one rule that covers all cases.

Field	Description
Source Address	Click Add to add source addresses, address groups, or regions (default is any). Select from the drop-down list, or click the Address , Address Group , or Regions link at the bottom of the drop-down list, and specify the settings. Select the Negate check box to choose any address except the configured ones.

Destination Tab

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

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

Protocol/Application Tab

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

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

Defining Captive Portal Policies

Policies > Captive Portal

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

Before defining captive portal policies, enable captive portal and configure captive portal settings on the **User Identification** page, as described in “[Configuring the Firewall for User Identification](#)”.

For configuration guidelines and information on other policy types, see “[Policies and Security Profiles](#)”.

The following tables describe the captive portal policy settings:

- [“General Tab”](#)
- [“Source Tab”](#)
- [“Destination Tab”](#)
- [“Service/URL Category Tab”](#)
- [“Action Tab”](#)

General Tab

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

Field	Description
Name	Enter a name to identify the rule (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.
Description	Enter a description for the rule (up to 255 characters).
Tag	If you need to tag the policy, click Add to specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.

Source Tab

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

Field	Description
Source	<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 the Negate check box to choose any address except the configured ones. Click Add to specify multiple interfaces or zones.

Destination Tab

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

Field	Description
Destination	<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 the Negate check box to choose any address except the configured ones. Click Add to specify multiple interfaces or zones.

Service/URL Category Tab

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

Field	Description
Service	<p>Select services to limit to specific TCP and/or UDP port numbers. Choose one of the following from the drop-down list:</p> <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. See “Services” and “Service Groups”.

Field	Description
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 list. You can add multiple categories. See “Dynamic Block Lists” for information on defining custom categories.

Action Tab

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

Field	Description
Action Setting	Choose an action to take: <ul style="list-style-type: none"> • web-form—Present a captive portal page for the user to explicitly enter authentication credentials. • no-captive-portal—Allow traffic to pass without presenting a captive portal page for authentication. • browser-challenge—Open an NT LAN Manager (NTLM) authentication request to the user's web browser. The web browser will respond using the user's current login credentials.

Defining DoS Policies

► *Policies > DoS Protection*

DoS protection policies allow you to control the number of sessions between interfaces, zones, addresses, and countries based on aggregate sessions or source and/or destination IP addresses. For example, you can control traffic to and from certain addresses or address groups, or from certain users and for certain services.

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

For information on defining policies on Panorama, see “[Defining Policies on Panorama](#)”.

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

General Tab

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

Field	Description
Name	Enter a name to identify the rule (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.

Field	Description
Description	Enter a description for the rule (up to 255 characters).
Tag	If you need to tag the policy, click Add to specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.

Source Tab

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

Field	Description
Source	<p>Specify the following information:</p> <ul style="list-style-type: none"> • Choose Interface from the Type drop-down list to apply the DoS policy to traffic coming from an interface or a group of interfaces. Choose Zone if the DoS policy needs to be applied to traffic coming from all interfaces in a given zone. Click Add to specify multiple interfaces or zones. • Specify the Source Address setting to apply the DoS policy for traffic coming from specific source addresses. Select the Negate check box to choose any address except the configured ones. Click Add to specify multiple addresses. • Specify the Source User setting to apply the DoS policy for traffic from specific users. The following source user types are supported: <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><i>Note: If you are using a RADIUS server and not the User-ID Agent, the list of users is not displayed, and you must enter user information manually.</i></p>

Destination Tab

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

Field	Description
Destination	<p>Specify the following information:</p> <ul style="list-style-type: none"> Choose Interface from the Type drop-down list to apply the DoS policy to traffic coming from an interface or a group of interfaces. Choose Zone if the DoS policy needs to be applied to traffic coming from all interfaces in a given zone. Click Add to specify multiple interfaces or zones. Specify the Destination Address setting to apply the DoS policy for traffic to specific destination addresses. Select the Negate check box to choose any address except the configured ones. Click Add to specify multiple addresses.

Options/Protection Tab

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

Field	Description
Service	Select from the drop-down list to apply the DoS policy to only the configured services.
Action	<p>Choose the action from the drop-down list:</p> <ul style="list-style-type: none"> Deny—Drop all traffic. Allow—Permit all traffic. Protect—Enforce protections supplied in the thresholds that are configured as part of the DoS profile applied to this rule.
Schedule	Select a pre-configured schedule from the drop-down list to apply the DoS rule to a specific date/time.
Log Forwarding	If you want to trigger forwarding of threat log entries to an external service—such as a syslog server or Panorama—select a log forwarding profile from the drop-down or click Profile to create a new one. Note that only traffic that matches an action in the rule will be logged and forwarded.
Aggregate	Select a DoS protection profile from the drop-down list to determine the rate at which you want to take action in response to DoS threats. The aggregate setting applies to the total of all traffic from the specified source to specified destination.

Field	Description
Classified	<p>Select the check box and specify the following:</p> <ul style="list-style-type: none"> • Profile—Select the profile from the drop-down list. • Address—Select whether to apply the rule to the source, destination, or source and destination IP addresses. <p>If a classified profile is specified, the profile limitations are applied to a source IP address, destination IP address, or source and destination IP address pair. For example, you could specify a classified profile with a session limit of 100 and specify an Address setting of “source” in the rule. The result would be a limit of 100 sessions at any given time for that particular source IP address.</p>

Security Profiles

Each security policy can include specification of one or more security profiles, which provide additional protection and control.

You can also add threat exceptions to Anti-spyware and Vulnerability profiles. To make management of threat exceptions easier, you can add threat exceptions directly from the **Monitor > Logs > Threat** list. Threat exceptions are usually configured when false-positives occur. In this case, you can set an exception on a threat until Palo Alto Networks releases a new signature for the given false-positive.

The following profile types are available:

- Antivirus profiles to protect against worms and viruses or block spyware downloads. See “[Antivirus Profiles](#)”.
- Anti-spyware profiles to block attempts by spyware to access the protected network. See “[Anti-spyware Profiles](#)”.
- Vulnerability protection profiles to stop attempts to exploit system flaws or gain unauthorized access to systems. See “[Vulnerability Protection Profiles](#)”.
- URL filtering profiles to restrict access to specific web sites and web site categories. See “[URL Filtering Profiles](#)”.
- File blocking profiles to block selected file types. See “[File Blocking Profiles](#)”.
- Data filtering profiles that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall. See “[Data Filtering Profiles](#)”.

In addition to individual profiles, you can create profile groups from **Objects > Security Profile Groups** to combine profiles that are often applied together.



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

You can choose from the following actions when defining antivirus and anti-spyware profiles.

- **Default**—Takes the default action that is specified internally in the signature for each threat.
- **Allow**—Permits the application traffic.

- **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
- **Block**—Drops the application traffic.

The following actions are available when defining custom Spyware and Vulnerability objects:

- **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
- **Drop Packets**—Keeps all packets from continuing past the firewall.
- **Reset Both**—Resets the client and server.
- **Reset Client**—Resets the client.
- **Reset Server**—Resets the server.
- **Block-IP**—This action blocks traffic from either a source or a source-destination pair (configurable) for a specified period of time.

Antivirus Profiles

► *Objects > Security Profiles > Antivirus*

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

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

For a list of all security profile types and the actions that can be taken on matched traffic, see “[Security Profiles](#)”.

The following tables describe the policy-based forwarding settings:

- “[Antivirus Profile Page](#)”
- “[Antivirus Tab](#)”
- “[Exceptions Tab](#)”

Antivirus Profile Page

Use this page to define a name and description for the profile.

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of antivirus profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Description	Enter a description for the profile (up to 255 characters).

Antivirus Tab

Use the Antivirus tab to define the type of traffic that will be inspected, such as ftp, and http, and then specify the action to take. You can define different actions for standard antivirus signatures (Action column) and signatures generated by the [WildFire](#) system (WildFire Action column). Some environments may have requirements for a longer soak time for antivirus signatures, so this option enables the ability to set different actions for the two antivirus signature types provided by Palo Alto Networks. For example, the standard antivirus signatures go through a longer soak period before being released (24 hours), versus WildFire signatures, which can be generated and released within 15 minutes after a threat is detected. Because of this, you may want to choose the alert action on WildFire signatures instead of blocking.

Use the **Applications Exception** table to define applications that will not be inspected. For example, you may want to allow http, but not inspect traffic from a specific application that operates over http.

Field	Description
Packet Capture	Select the check box if you want to capture identified packets.
Decoders and Actions	For each type of traffic that you want to inspect for viruses, select an action from the drop-down list. You can also take specific action based on signatures created by WildFire .
Applications Exceptions and Actions	<p>Identify applications that will be exceptions to the antivirus rule. For example, to block all HTTP traffic except for a specific application, you can define an antivirus profile for which the application is an exception. Block is the action for the HTTP decoder, and Allow is the exception for the application.</p> <p>To find an application, start typing the application name in the text box. A matching list of applications is displayed, and you can make a selection. The application is added to the table, and you can assign an action.</p> <p>For each application exception, select the action to be taken when the threat is detected.</p>

Exceptions Tab

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

Field	Description
Threat ID	Add specific threats that should be ignored. Exceptions that are already specified are listed. You can add additional threats by entering the threat ID and clicking Add . Threat IDs are presented as part of the threat log information. See "Viewing the Logs" .

Anti-spyware Profiles

► *Objects > Security Profiles > Anti-spyware*

A security policy can include specification of an anti-spyware profile for “phone home” detection (detection of traffic from installed spyware). The default anti-spyware profile detects phone-home protection for all severity levels except the low and informational levels. Customized profiles can be used to minimize anti-spyware 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.

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 **DNS Signatures** settings provides an additional method of identifying infected hosts on a network. These signatures detect specific DNS lookups for host names that have been associated with malware. The DNS signatures can be configured to allow, alert, or (default) block when these queries are observed, just as with regular antivirus signatures. Additionally, hosts that perform DNS queries for malware domains will appear in the botnet report. DNS signatures are downloaded as part of the antivirus updates.

The **Anti-spyware** page presents a default set of columns. Additional columns of information are available by using the column chooser. Click the arrow to the right of a column header and select the columns from the Columns sub-menu. For more information, see ["Using Tables on Configuration Pages"](#).

The following tables describe the anti-spyware profile settings:

Table 145. Anti-spyware Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of anti-spyware profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Description	Enter a description for the profile (up to 255 characters).

Table 145. Anti-spyware Profile Settings (Continued)

Field	Description
Shared	<p>Select this check box if you want the Anti-Spyware profile to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the Virtual System drop-down (Objects > Security Profiles > Anti-Spyware page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Anti-Spyware Profile dialog. • All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the Device Group drop-down (Objects > Security Profiles > Anti-Spyware page). <p>After you save the profile, you cannot change its Shared setting. The Objects > Security Profiles > Anti-Spyware page shows the current setting in the Location field.</p>
Rules Tab	
Rule Name	Specify the rule name.
Threat Name	Enter any to match all signatures, or enter text to match any signature containing the entered text as part of the signature name.
Severity	Choose a severity level (critical , high , medium , low , or informational).
Action	Choose an action (Default , Alert , Allow , or Drop) for each threat.
Packet Capture	<p>Select the check box if you want to capture identified packets. Select single-packet to capture one packet when a threat is detected, or select the extended-capture option to capture from 1 to 50 packets. Extended-capture will provide much more context to the threat when analyzing the threat logs. To view the packet capture, navigate to Monitor > Logs > Threat and locate the log entry you are interested in and then click the green down arrow in the second column. To define the number of packets that should be captured, navigate to Device > Setup > Content-ID and then edit the Threat Detection Settings section.</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	
Exceptions	<p>Select the Enable check box for each threat for which you want to assign an action, or select All to respond to all listed threats. The list depends on the selected host, category, and severity. If the list is empty, there are no threats for the current selections.</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	

Table 145. Anti-spyware Profile Settings (Continued)

Field	Description
Action on DNS queries	<p>Choose an action to be taken when DNS lookups are made to known malware sites (Alert, Allow, sinkhole, or default (Block)).</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 (i.e. the firewall cannot see the originator of the DNS query). When a threat prevention license is installed and an anti-spyware profile is enabled in a security profile, the DNS-based signatures will trigger on DNS queries directed at malware domains. In a typical deployment where the firewall is north of the local DNS server, the threat log will identify the local DNS resolver as the source of the traffic rather than the actual infected host. Sinkholing malware DNS queries solves this visibility problem by forging responses to the queries directed at malicious domains, so that clients attempting to connect to malicious domains (for command-and-control, for example) instead attempt connections to an IP address specified by the administrator. Infected hosts can then be easily identified in the traffic logs because any host that attempts to connect to the sinkhole IP are most likely infected with malware.</p> <p>After selecting the sinkhole action, specify an IPv4 and/or IPv6 address that will be used as the sinkhole (the default is the loopback IP, which will resolve domains to the local host). When a sinkhole IP address is configured, the infected clients can be identified by filtering the traffic logs or by building a custom report that checks for sessions to the specified IP address. It is important to choose an IP address that results in a session having to be routed through the firewall in order for the firewall to see the session, for example an unused IP in another internal zone.</p> <p>The following is the sequence of events that will occur when the sinkhole feature is enabled:</p> <ol style="list-style-type: none"> 1. Malicious software on an infected client computer sends a DNS query to resolve a malicious host on the Internet. 2. The client's DNS query is sent to an internal DNS server, which then queries a public DNS server on the other side of the firewall. 3. The DNS query matches a DNS entry in the DNS signatures database, so the sinkhole action will be performed on the query. 4. The infected client then attempts to start a session with the host, but uses the forged IP address instead. The forged IP address is the address defined in the Anti-Spyware profile DNS Signatures tab when the sinkhole action is selected. 5. The administrator is alerted of a malicious DNS query in the threat log, and can then search the traffic logs for the sinkhole IP address and can easily locate the client IP address that is trying to start a session with the sinkhole IP address.
Packet Capture	Select the check box if you want to capture identified packets.

Table 145. Anti-spyware Profile Settings (Continued)

Field	Description
Enable Passive DNS Monitoring	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 (i.e. originating from the local recursive resolver, not individual clients) DNS query and response packet payloads. This information is used by the Palo Alto Networks threat research team to gain insights into malware propagation and evasion techniques that abuse the DNS system. Information gathered through this data collection is used to improve accuracy and malware detection abilities within PAN-DB URL filtering, DNS-based command-and-control signatures, and WildFire. The recommended setting for this feature is to enable it. <i>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.</i>
Threat ID	The option is disabled by default. Manually enter DNS signature exceptions (range 4000000-4999999).

Vulnerability Protection Profiles

► *Objects > Security Profiles > Vulnerability Protection*

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

- The **default** profile applies the default action to all client and server critical, high, and medium severity 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, see “[Defining Security Policies](#)”.

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

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

The **Vulnerability Protection** page presents a default set of columns. Additional columns of information are available by using the column chooser. Click the arrow to the right of a column header and select the columns from the Columns sub-menu. For more information, see “[Using Tables on Configuration Pages](#)”.

The following tables describe the vulnerability protection profile settings:

Table 146. Vulnerability Protection Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of vulnerability protection profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared	Select this check box if you want the Vulnerability Protection profile to be available to: <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the Virtual System drop-down (Objects > Security Profiles > Vulnerability Protection page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Vulnerability Protection Profile dialog. All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the Device Group drop-down (Objects > Security Profiles > Vulnerability Protection page). After you save the profile, you cannot change its Shared setting. The Objects > Security Profiles > Vulnerability Protection page shows the current setting in the Location field.
Rules Tab	
Rule Name	Specify a name to identify the rule.
Threat Name	Specify a text string to match. The firewall applies a collection of signatures to the rule by searching signature names for this text string.
Action	Choose the action (Alert , Allow , Default , or Block) to take when the rule is triggered. 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.
Host	Specify whether to limit the signatures for the rule to those that are client side, server side, or either (any).
Packet Capture	Select the check box if you want to capture identified packets. Select single-packet to capture one packet when a threat is detected, or select the extended-capture option to capture from 1 to 50 packets. Extended-capture will provide much more context to the threat when analyzing the threat logs. To view the packet capture, navigate to Monitor > Logs > Threat and locate the log entry you are interested in and then click the green down arrow in the second column. To define the number of packets that should be captured, navigate to Device > Setup > Content-ID and then edit the Threat Detection Settings section. Packet captures will only occur if the action is allow or alert. If the block action is set, the session is ended immediately.

Table 146. Vulnerability Protection Profile Settings (Continued)

Field	Description
Category	Select a vulnerability category if you want to limit the signatures to those that match that category.
CVE List	Specify common vulnerabilities and exposures (CVEs) if you want to limit the signatures to those that also match the specified CVEs. Each CVE is in the format CVE- <i>yyyy</i> - <i>xxxx</i> , where <i>yyyy</i> is the year and <i>xxxx</i> is the unique identifier. You can perform a string match on this field. For example, to find vulnerabilities for the year 2011, enter "2011".
Vendor ID	Specify vendor IDs if you want to limit the signatures to those that also match the specified vendor IDs. For example, the Microsoft vendor IDs are in the form MS <i>yy</i> - <i>xxx</i> , where <i>yy</i> is the two-digit year and <i>xxx</i> is the unique identifier. For example, to match Microsoft for the year 2009, enter "MS09".
Severity	Select severities to match (informational , low , medium , high , or critical) if you want to limit the signatures to those that also match the specified severities.
Exceptions Tab	
Threats	<p>Select the Enable check box for each threat for which you want to assign an action, or select All to respond to all listed threats. The list depends on the selected host, category, and severity. If the list is empty, there are no threats for the current selections.</p> <p>Choose an action from the drop-down list box, or choose from the Action drop-down at the top of the list to apply the same action to all threats. If the Show All check box is selected, all signatures are listed. If the Show All check box is not selected, only the signatures that are exceptions are listed.</p> <p>Select the Packet Capture check box 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 the pencil icon  next to the threat name on the Vulnerability tab (with the Custom option selected). You can specify the number of hits per unit of time and whether the threshold applies to source, destination, or source-and-destination.</p> <p>Thresholds can be applied on a source IP, destination IP or a combination of source IP and destination IP.</p> <p><i>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.</i></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>

URL Filtering Profiles

► *Objects > Security Profiles > URL Filtering*

A security policy can include specification of a URL filtering profile that blocks access to specific web sites and web site categories, enforces safe search, or generates an alert when the specified web sites are accessed (a URL filtering license is required). You can also define a “block list” of web sites that are always blocked (or generate alerts) and an “allow list” of web sites that are always allowed.

To apply URL filtering profiles to security policies, see “[Defining Security Policies](#)”. To create custom URL categories with your own lists of URLs, see “[Dynamic Block Lists](#)”.

The following tables describe the URL filtering profile settings:

Table 147. URL Filtering Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of URL filtering profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared	Select this check box if you want the URL Filtering profile to be available to: <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the Virtual System drop-down (<i>Objects > Security Profiles > URL Filtering</i> page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the URL Filtering Profile dialog. All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the Device Group drop-down (<i>Objects > Security Profiles > URL Filtering</i> page). After you save the profile, you cannot change its Shared setting. The <i>Objects > Security Profiles > URL Filtering</i> page shows the current setting in the Location field.
Categories	
(Configurable for BrightCloud only) Action on License Expiration	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. <p><i>Note: If you are using the BrightCloud database and you set this option to Block upon license expiration, all URLs will be blocked, not just the URL categories that are set to block. If you set to Allow, all URLs will be allowed.</i></p> <p><i>If you are using PAN-DB, URL filtering will continue to function and the URL categories that are currently in cache will be used to either block or allow based on your configuration.</i></p>

Table 147. URL Filtering Profile Settings (Continued)

Field	Description						
Block List	<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>IMPORTANT: 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> <pre> / ? & = ; + </pre> <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-collapse: collapse;"> <tr> <td style="width: 30%;">*.yahoo.com</td> <td style="width: 70%; text-align: right;">(Tokens are: “*”, “yahoo” and “com”)</td> </tr> <tr> <td>www.*.com</td> <td style="text-align: right;">(Tokens are: “www”, “*” and “com”)</td> </tr> <tr> <td>www.yahoo.com/search=*</td> <td style="text-align: right;">(Tokens are: “www”, “yahoo”, “com”, “search”, “*”)</td> </tr> </table> <p>The following patterns are invalid because the character “*” is not the only character in the token.</p> <p style="margin-left: 40px;"><i>ww*.yahoo.com</i> <i>www.y*.com</i></p>	*.yahoo.com	(Tokens are: “*”, “yahoo” and “com”)	www.*.com	(Tokens are: “www”, “*” and “com”)	www.yahoo.com/search=*	(Tokens are: “www”, “yahoo”, “com”, “search”, “*”)
.yahoo.com	(Tokens are: “”, “yahoo” and “com”)						
www.*.com	(Tokens are: “www”, “*” and “com”)						
www.yahoo.com/search=*	(Tokens are: “www”, “yahoo”, “com”, “search”, “*”)						
Action	<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. See Table 1 in the “Defining Management Settings”. 						

Table 147. URL Filtering Profile Settings (Continued)

Field	Description						
Allow List	<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> <p>IMPORTANT: You must omit the “http and https” portion of the URLs when adding web sites to the list.</p> <p>Entries in the allow list are an exact match and are case-insensitive. For example, “www.paloaltonetworks.com” is different from “paloaltonetworks.com”. If you want to allow the entire domain, you should include both “*.paloaltonetworks.com” and “paloaltonetworks.com”.</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> <pre> . / ? & = ; + </pre> <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-collapse: collapse;"> <tr> <td style="width: 30%;">*.yahoo.com</td> <td>(Tokens are: “*”, “yahoo” and “com”)</td> </tr> <tr> <td>www.*.com</td> <td>(Tokens are: “www”, “*” and “com”)</td> </tr> <tr> <td>www.yahoo.com/search=*</td> <td>(Tokens are: “www”, “yahoo”, “com”, “search”, “*”)</td> </tr> </table> <p>The following patterns are invalid because the character “*” is not the only character in the token.</p> <p style="margin-left: 40px;">ww*.yahoo.com</p> <p style="margin-left: 40px;">www.y*.com</p> <p>This list takes precedence over the selected web site categories.</p>	*.yahoo.com	(Tokens are: “*”, “yahoo” and “com”)	www.*.com	(Tokens are: “www”, “*” and “com”)	www.yahoo.com/search=*	(Tokens are: “www”, “yahoo”, “com”, “search”, “*”)
.yahoo.com	(Tokens are: “”, “yahoo” and “com”)						
www.*.com	(Tokens are: “www”, “*” and “com”)						
www.yahoo.com/search=*	(Tokens are: “www”, “yahoo”, “com”, “search”, “*”)						
Category/Action	<p>For each category, select the action to take when a web site of that category 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. • allow—Allow the user to access the web site. • block—Block access to the web site. • continue—Allow the user to access the blocked page by clicking Continue on the block page. • override—Allow the user to access the blocked page after entering a password. The password and other override settings are specified in the URL Admin Override area of the Settings page. See Table 11 in the “Defining Management Settings”. <p>Note: The Continue and Override pages will not be displayed properly on client machines that are configured to use a proxy server.</p>						

Table 147. URL Filtering Profile Settings (Continued)

Field	Description
Check URL Category	Click to access the web site where you can enter a URL or IP address to view categorization information.
Dynamic URL Filtering Default: Disabled (Configurable for BrightCloud only)	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." <i>With PAN-DB, this option is enabled by default and is not configurable.</i>
Log container page only Default: Enabled	Select the check box to log only the URLs that match the content type that is specified.
Enable Safe Search Enforcement Default: Disabled To use this feature, a URL filtering license is not required.	Select this check box to enforce strict safe search filtering. When enabled, this option will prevent users who are searching the Internet using one of the following search providers—Bing, Google, Yahoo, Yandex, or YouTube—from viewing the search results unless the strictest safe search option is set in their browsers for these search engines. If a user performs a search using one of these search engines and their browser or search engine account setting for safe search is not set to strict, the search results will be blocked (depending on the action set in the profile) and the user will be prompted to set their safe search setting to strict. <i>Note: If you are performing a search on Yahoo Japan (yahoo.co.jp) while logged into your Yahoo account, the lock option for the search setting must also be enabled.</i> To enforce safe search, the profile must be added to a security policy. And, to enable safe search for encrypted sites (HTTPS), the profile must be attached to a decryption policy. The ability of the firewall to detect the safe search setting within these three providers will be updated using the Applications and Threats signature update. If a provider changes the safe search setting method that Palo Alto Networks uses to detect the safe search settings, an update will be made to the signature update to ensure that the setting is detected properly. Also, the evaluation to determine whether a site is judged to be safe or unsafe is performed by each search provider, not Palo Alto Networks. To prevent users from bypassing this feature by using other search providers, configure the URL filtering profile to block the search-engines category and then allow access to Bing, Google, Yahoo, Yandex, and YouTube. See the PAN-OS Administrator's Guide for more information.

Table 147. URL Filtering Profile Settings (Continued)

Field	Description
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.

File Blocking Profiles

► *Objects > Security Profiles > File Blocking*

A security policy can include specification of a file blocking profile that blocks selected file types from being uploaded and/or downloaded, or generates an alert when the specified file types are detected. If the **forward** action is selected, supported file types will be sent to **WildFire** where they will be analyzed for malicious behavior. Table 149 lists the supported file formats at the time of this publication. However, because new file type support can be added in a content update, for the most up-to-date list, click **Add** in the **File Types** field of the File Blocking Profile dialog.

To apply file blocking profiles to security policies, see “[Defining Security Policies](#)”.

The following tables describe the file blocking profile settings:

Table 148. File Blocking Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of file blocking profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the profile (up to 255 characters).

Table 148. File Blocking Profile Settings (Continued)

Field	Description
Shared	<p>Select this check box if you want the File Blocking profile to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the Virtual System drop-down (Objects > Security Profiles > File Blocking page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the File Blocking Profile dialog. • All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the Device Group drop-down (Objects > Security Profiles > File Blocking page). <p>After you save the profile, you cannot change its Shared setting. The Objects > Security Profiles > File Blocking page shows the current setting in the Location field.</p>
Rules	<p>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:</p> <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—Select the file types for which you want to block or generate alerts. • Direction—Select the direction of the file transfer (Upload, Download, or Both). • Action—Select the action taken when the selected file types are detected: <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. <p><i>When you create a file blocking profile with the action continue or continue-and-forward (used for WildFire forwarding), you can only choose the application web-browsing. If you choose any other application, traffic that matches the security policy will not flow through the firewall due to the fact that the users will not be prompted with a continue page.</i></p> <ul style="list-style-type: none"> – forward—The file is automatically sent to WildFire. – continue-and-forward—A continue page is presented, and the file is sent to WildFire (combines the continue and forward actions). This action only works with web-based traffic. This is due to the fact that a user must click continue before the file will be forward and the continue response page option is only available with http/https.

Table 149. Supported File Formats for File Blocking

Field	Description
apk	Android application package file
avi	Video file based on Microsoft AVI (RIFF) file format
avi-divx	AVI video file encoded with the DivX codec
avi-xvid	AVI video file encoded with the XviD codec
bat	MS DOS Batch file
bmp-upload	Bitmap image file (upload only)
cab	Microsoft Windows Cabinet archive file
cdr	Corel Draw file
class	Java bytecode file
cmd	Microsoft command file
dll	Microsoft Windows Dynamic Link Library
doc	Microsoft Office Document
docx	Microsoft Office 2007 Document
dpx	Digital Picture Exchange file
dsn	Database Source Name file
dwf	Autodesk Design Web Format file
dwg	Autodesk AutoCAD file
edif	Electronic Design Interchange Format file
email-link	<p>By forwarding the email-link file type, the firewall extracts HTTP/HTTPS links contained in SMTP and POP3 email messages and forward the links to the WildFire cloud for analysis (this feature is not supported on the WF-500 WildFire appliance). Note that the firewall only extracts links and associated session information (sender, recipient, and subject) from the email messages that traverse the firewall; it does not receive, store, forward, or view the email message.</p> <p>After receiving an email link from a firewall, WildFire visits the links to determine if the corresponding web page hosts any exploits. If it determines that the page itself is benign, no log entry will be sent to the firewall. If the link is malicious, a WildFire detailed analysis report is generated in the firewall's WildFire Submissions log and the URL is added to PAN-DB.</p>
encrypted-doc	Encrypted Microsoft Office Document
encrypted-docx	Encrypted Microsoft Office 2007 Document
encrypted-office2007	Encrypted Microsoft Office 2007 Document
encrypted-pdf	Encrypted Adobe PDF Document
encrypted-ppt	Encrypted Microsoft Office PowerPoint
encrypted-pptx	Encrypted Microsoft Office 2007 PowerPoint
encrypted-rar	Encrypted rar file
encrypted-xls	Encrypted Microsoft Office Excel

Table 149. Supported File Formats for File Blocking (Continued)

Field	Description
encrypted-xlsx	Encrypted Microsoft Office 2007 Excel
encrypted-zip	Encrypted zip file
exe	Microsoft Windows Executable
flash	Includes the Adobe Shockwave Flash SWF and SWC file types. The SWF file delivers vector graphics, text, video, and sound over the Internet and the content is viewed using the Adobe Flash player. The SWC file is a compressed package of SWF components.
flv	Adobe Flash Video file
gds	Graphics Data System file
gif-upload	GIF image file (upload only)
gzip	Files compressed with gzip utility
hta	HTML Application file
iso	Disc Image file based on ISO-9660 standard
iwork-keynote	Apple iWork Keynote documents
iwork-numbers	Apple iWork Numbers documents
iwork-pages	Apple iWork Pages documents
jar	Java ARchive
jpeg-upload	JPG/JPEG image file (upload only)
lnk	Microsoft Windows file shortcut
lzh	File compressed with lha/lzh utility/algorithm
mdb	Microsoft Access Database file
mdi	Microsoft Document Imaging file
mkv	Matroska Video file
mov	Apple Quicktime Movie file
mp3	MP3 audio file
mp4	MP4 audio file
mpeg	Movie file using MPEG-1 or MPEG-2 compression
msi	Microsoft Windows Installer package file
msoffice	Microsoft Office File (doc, docx, ppt, ppts, pub, pst, rtf, xls, xlsx). If you want the firewall to block/forward MS Office files, it is recommended that you select this "msoffice" group to ensure all supported MS Office file types will be identified instead of selecting each file type individually.
ocx	Microsoft ActiveX file
pdf	Adobe Portable Document file
PE	Microsoft Windows Portable Executable (exe, dll, com, scr, ocx, cpl, sys, drv, tlb)
pgp	Security key or digital signature encrypted with PGP software

Table 149. Supported File Formats for File Blocking (Continued)

Field	Description
pif	Windows Program Information File containing executable instructions
pl	Perl Script file
png-upload	PNG image file (upload only)
ppt	Microsoft Office PowerPoint Presentation
pptx	Microsoft Office 2007 PowerPoint Presentation
psd	Adobe Photoshop Document
rar	Compressed file created with winrar
reg	Windows Registry file
rm	RealNetworks Real Media file
rtf	Windows Rich Text Format document file
sh	Unix Shell Script file
stp	Standard for the Exchange of Product model data 3D graphic file
tar	Unix tar archive file
tdb	Tanner Database (www.tannereda.com)
tif	Windows Tagged Image file
torrent	BitTorrent file
wmf	Windows Metafile to store vector images
wmv	Windows Media Video file
wri	Windows Write document file
wsf	Windows Script file
xls	Microsoft Office Excel
xlsx	Microsoft Office 2007 Excel
zcompressed	Compressed Z file in Unix, decompressed with uncompress
zip	Winzip/pkzip file

Data Filtering Profiles

► *Objects > Security Profiles > Data Filtering*

A security policy can include specification of a data filtering profile to help identify sensitive information such as credit card or social security numbers and prevent the sensitive information from leaving the area protected by the firewall.

To apply data filtering profiles to security policies, see “[Defining Security Policies](#)”.

The following tables describe the data filtering profile settings:

Table 150. Data Filtering Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of log forwarding profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared	Select this check box if you want the Data Filtering profile to be available to: <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the Virtual System drop-down (<i>Objects > Security Profiles > Data Filtering</i> page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Data Filtering Profile dialog. All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the Device Group drop-down (<i>Objects > Security Profiles > Data Filtering</i> page). After you save the profile, you cannot change its Shared setting. The <i>Objects > Security Profiles > Data Filtering</i> page shows the current setting in the Location field.
Data Capture	Select the check box to automatically collect the data that is blocked by the filter.



Specify a password for Manage Data Protection on the *Settings* page to view your captured data. See “[Defining Management Settings](#)”.

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

Table 151. Data Pattern Settings

Field	Description
Data Pattern	<p>Choose an existing data pattern from the Data Pattern drop-down list, or configure a new pattern by choosing Data Pattern from the list and specifying the following information:</p> <ul style="list-style-type: none"> • Name—Configure a name for the data pattern. • Description—Configure a description for the data pattern. • Shared—Select this option if the data pattern object will be shared across multiple virtual systems. • Weight—Specify unit values for the specified patterns to use in calculating thresholds. For instance, if you designate a weight of 5 for SSN#, every instance of a SSN pattern will increment the threshold by 5. In other words, the detection of ten SSN patterns will result in 10×5 (weight) = 50. <ul style="list-style-type: none"> – CC#—Specify a weight for the credit card field (range 0-255). – SSN#—Specify a weight for the social security number field, where the field includes dashes, such as 123-45-6789 (range 0-255, 255 is highest weight). – SSN# (without dash)—Specify a weight for the social security number field, where the entry is made without dashes, such as 123456789 (range 0-255, 255 is highest weight). • Custom Patterns—To match a custom data pattern for the traffic that is subject to this profile, create a custom data pattern by clicking Add and specifying the pattern name, regular expression (regex) to match, and weight (0-255, 255 is highest weight). You can add multiple match expressions to the same data pattern profile.
Applications	<p>Specify the applications to include in the filtering rule:</p> <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	<p>Specify the file types to include in the filtering rule:</p> <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.
Direction	<p>Specify whether to apply the filter in the upload direction, download direction, or both.</p>
Alert Threshold	<p>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 ($20 \text{ instances} \times 5 \text{ weight} = 100$).</p>
Block Threshold	<p>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 ($20 \text{ instances} \times 5 \text{ weight} = 100$).</p>

DoS Profiles

► *Objects > Security Profiles > DoS Protection*

DoS protection profiles are designed for high precision targeting and augment zone protection profiles. The DoS profile specifies the types of actions and the matching criteria to detect a DoS attack. These profiles are attached to DoS protection policies to allow you to control traffic between interfaces, zones, addresses, and countries based on aggregate sessions or unique source and/or destination IP addresses. To apply DoS profiles to DoS policies, see “[Defining DoS Policies](#)”.



If you have a multi virtual system environment, and have enabled the following:

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

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

- SYN cookies
- IP fragmentation
- ICMPv6

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

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

The following tables describe the DoS protection profile settings:

Table 152. DoS Protection Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of log forwarding profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	<p>Select this check box if you want the DoS Protection profile to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the Virtual System drop-down (Objects > Security Profiles > DoS Protection page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the DoS Protection Profile dialog. • All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the Device Group drop-down (Objects > Security Profiles > DoS Protection page). <p>After you save the profile, you cannot change its Shared setting. The Objects > Security Profiles > DoS Protection page shows the current setting in the Location field.</p>
Description	Enter a description of the profile (up to 255 characters).
Type	<p>Specify one of the following profile types:</p> <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 rule with a SYN flood threshold of 10000 packets per second (pps) counts all packets that hit that particular DoS rule. • classified—Apply the DoS thresholds configured in the profile to all packets satisfying the classification criterion (source IP, destination IP or source-and-destination IP).

Table 152. DoS Protection Profile Settings (Continued)

Field	Description
Flood Protection Tab	
Syn Flood subtab	Select the check box to enable the type of flood protection indicated on the tab, and specify the following settings:
UDP Flood subtab	
ICMP Flood subtab	
Other subtab	<ul style="list-style-type: none"> • Action—(SYN Flood only) Choose from the following options: <ul style="list-style-type: none"> – Random Early Drop—Drop packets randomly before the overall DoS limit is reached. – SYN cookies—Use SYN cookies to generate acknowledgments so that it is not necessary to drop connections in the presence of a SYN flood attack. • Alarm Rate—Specify the rate (pps) at which a DoS alarm is generated. (Range is 0-2000000 pps; default is 10000 pps). • Activate Rate—Specify the threshold rate (pps) at which a DoS response is activated. The DoS response is configured in the Action field of the DoS policy where this profile is referenced. When the Activate Rate threshold is reached, Random Early Drop occurs. (Range is 0-2000000 pps; default is 10000 pps). • Max Rate—Specify the threshold rate of incoming packets per second the firewall allows. When the threshold is exceeded, new packets that arrive are dropped and the Action in the DoS policy is triggered. (Range is 2-2000000 pps; default is 40000 pps.) • Block Duration—Specify the length of time (seconds) during which the offending packets will be denied. Packets arriving during the block duration do not count towards triggered alerts. (Range is 1-21600 seconds; default is 300 seconds.) <p><i>Note: When defining packets per second (pps) thresholds limits for zone and DoS protection profiles, the threshold is based on the packets per second that do not match a previously established session.</i></p>
Resources Protection Tab	
Sessions	Select the check box to enable resources protection.
Max Concurrent Limit	Specify the maximum number of concurrent sessions. If the DoS profile type is aggregate, this limit applies to the entire traffic hitting the DoS rule on which the DoS profile is applied. If the DoS profile type is classified, this limit applies to the entire traffic on a classified basis (source IP, destination IP or source-and-destination IP) hitting the DoS rule on which the DoS profile is applied.

Other Policy Objects

Policy objects are the elements that enable you to construct, schedule, and search for policies. The following element types are supported:

- Addresses and address groups to determine the scope of the policy. See “[Defining Address Groups](#)”.
- Applications and application groups that allow you to specify how software applications are treated in policies. See “[Applications and Application Groups](#)”.

- Application filters that allow you to simplify searches. See “[Application Filters](#)”.
- Services and service groups to limit the port numbers. See “[Services](#)”.
- Tags to sort and filter objects. See “[Working with Tags](#)”.
- Data patterns to define categories of sensitive information for data filtering policies. See “[Data Patterns](#)”.
- Custom URL categories that contain your own lists of URLs to include as a group in URL filtering profiles. See “[Dynamic Block Lists](#)”.
- Spyware and vulnerability threats to allow for detailed threat responses. See “[Security Profile Groups](#)”.
- Log forwarding to specify log settings. See “[Log Forwarding](#)”.
- Schedules to specify when policies are active. See “[Schedules](#)”.

Defining Address Objects

► *Objects > Addresses*

An address object can include an IPv4 or IPv6 address (single IP, range, subnet) or a FQDN. It allows you to reuse the same object as a source or destination address across all the policy rulebases without having to add it manually each time. It is configured using the web interface or the CLI and a commit operation is required to make the object a part of the configuration.

To define an address object, click **Add** and fill in the following fields:

Table 153. New Address Settings

Field	Description
Name	Enter a name that describes the addresses to be defined (up to 63 characters). This name appears in the address list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	<p>Select this check box if you want the address object to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the object will be available only to the vsys selected in the Virtual System drop-down (Objects > Addresses page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Address dialog. • All device groups on Panorama. If you clear the check box, the object will be available only to the device group selected in the Device Group drop-down (Objects > Addresses page). <p>After you save the object, you cannot change its Shared setting. The Objects > Addresses page shows the current setting in the Location field.</p>
Description	Enter a description for the object (up to 255 characters).

Table 153. New Address Settings (Continued)

Field	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 using the following notation: <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>Example: “192.168.80.150/32” indicates one address, and “192.168.80.0/24” indicates all addresses from 192.168.80.0 through 192.168.80.255.</p> <p>Example: “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 DNS proxy object, if a proxy is configured. For information about DNS proxy, see “DNS Proxy”.</p>
Tags	<p>Select or enter the tags that you wish to apply to this address object.</p> <p>You can define a tag here or use the Objects > Tags tab to create new tags. For information on tags, see “Working with Tags”.</p>

Defining Address Groups

► *Objects > Address Groups*

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

- **Dynamic Address Groups:** A dynamic address group populates its members dynamically using lookups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover

setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall.

Unlike a static address group where you specify the network address of a host, the members of a dynamic address group are populated using a match criteria that you define. The match criteria uses logical *and* or *or* operators; each host that you want to add to the dynamic address group must bear the tag or attribute that is defined in the match criteria. Tags can be defined directly on the firewall or on Panorama or they can be dynamically defined using the XML API and registered with the firewall. When an IP address and the corresponding tag (one or more) is registered, each dynamic group evaluates the tags and updates the list of members in its group.

In order to register new IP address and tags or changes to current IP addresses and tags, you must use scripts that call the XML API on the firewall. If you have a virtual environment with VMware, instead of using scripts calling the XML API, you can use the VM Information Sources feature (**Device > VM Information Sources** tab) to configure the firewall to monitor the ESX(i) host or the vCenterServer and retrieve information (network address and corresponding tags) on new servers/guests deployed on these virtual machines.

In order to use a dynamic address group in policy you must complete the following tasks:

- Define a dynamic address group and reference it in a policy rule.
- Notify the firewall of the IP addresses and the corresponding tags, so that members of the dynamic address group can be formed. This can be done either using external scripts that use the XML API on the firewall or for a VMware-based environment it can be configured on the **Device > VM Information Sources** tab on the firewall.

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

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

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

Table 154. Address Group

Field	Description
Name	Enter a name that describes the address group (up to 63 characters). This name appears in the address list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this check box if you want the address group object to be available to: <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the object will be available only to the vsys selected in the Virtual System drop-down (Objects > Address Groups page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Address Group dialog. All device groups on Panorama. If you clear the check box, the object will be available only to the device group selected in the Device Group drop-down (Objects > Address Groups page). After you save the object, you cannot change its Shared setting. The Objects > Address Groups page shows the current setting in the Location field.
Description	Enter a description for the object (up to 255 characters).
Type	Select Static or Dynamic . <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><i>Note: To view the list of attributes for the match criteria, you must have configured the firewall to access and retrieve the attributes from the source/host. Each virtual machine on the configured information source(s), is registered with the firewall, and the firewall can poll the machine to retrieve changes in IP address or configuration without any modifications on the firewall.</i></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 " Working with Tags ".

Defining Regions

► *Objects > Regions*

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

The following tables describe the region settings:

Table 155. New Region Settings

Field	Description
Name	Enter a name that describes the region (up to 31 characters). This name appears in the address list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Geo Location	To specify latitude and longitude, select the check box and values (xxx.xxxxxx format). This information is used in the traffic and threat maps for App-Scope. See “Using App Scope”.
Addresses	Specify an IP address, range of IP addresses, or subnet to identify the region, using any of the following formats: <i>x.x.x.x</i> <i>x.x.x.x-y.y.y.y</i> <i>x.x.x.x/n</i>

Applications and Application Groups

► Objects > Applications

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. The number to the left of each entry represents the total number of applications with that attribute.

The firewall looks for the custom-defined patterns in network traffic and takes the specified action for the application.



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

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

- To apply application filters, click an item that you want to use as a basis for filtering. For example, to restrict the list to the Networking category, click **Networking** and the list will only show networking applications.

Category	Subcategory	Technology	Risk	Characteristic
241 business-systems	31 audio-streaming	476 browser-based	317 1	499 Evasive
333 collaboration	11 auth-service	452 client-server	242 2	394 Excessive Bandwidth
196 general-internet	15 database	197 network-protocol	294 3	264 Prone to Misuse
173 media	56 email	117 peer-to-peer	258 4	612 Transfers Files
299 networking	33 encrypted-tunnel		133 5	249 Tunnels Other Apps
2 unknown	19 erp-crm			266 Used by Malware
	154 file-sharing			733 Vulnerability
	46 gaming			779 Widely used

- To filter on additional columns, select an entry in the other columns. The filtering is successive: first category filters are applied, then subcategory filters, then technology filters, then risk, and finally characteristic filters.
- For example, the next figure shows the result of applying a category, subcategory, and risk filter. In applying the first two filters, the Technology column is automatically restricted to the technologies that are consistent with the selected category and sub category, even though a technology filter has not been explicitly applied.
- Each time a filter is applied, the list of applications in the lower part of the page is automatically updated, as shown in the following figure. Any saved filters can be viewed in **Objects > Application Filters**.

Search <input type="text"/>		<input type="checkbox"/> Custom Only	<input checked="" type="checkbox"/> Clear Filters	5 matching applications
Category ▲	Subcategory ▲	Technology ▲	Risk ▲	Characteristic ▲
5 collaboration	56 email 91 instant-messaging 30 internet-conferencing 5 social-business	5 browser-based	2 1 2	4 Transfers Files 1 Tunnels Other Apps 4 Vulnerability 2 Widely used
	64 social-networking 52 voip-video 35 web-posting			
Name	Category	Subcategory	Risk	Technology
blackboard	collaboration	social-business		browser-based
clearspace	collaboration	social-business		browser-based
projectplace	collaboration	social-business		browser-based
ripple	collaboration	social-business		browser-based
sharepoint (1 out of 6 shown)	collaboration	social-business		browser-based
sharepoint-base	collaboration	social-business		browser-based

- To search for a specific application, enter the application name or description in the **Search** field, and press **Enter**. The application is listed, and the filter columns are updated to show statistics for the applications that matched the search.

A search will match partial strings. When you define security policies, you can write rules that apply to all applications that match a saved filter. Such rules are dynamically updated when a new application is added through a content update that matches the filter.

- To view additional details about the application or to customize risk and timeout values, as described in the following table, click an application name. If the icon to the left of the application name has a yellow pencil on it, the application is a custom application. Note that the settings available vary by application.

The following tables describe the application settings:

Table 156. Application Details

Item	Description
Name	Name of the application.
Description	Description of the application (up to 255 characters).
Additional Information	Links to web sources (Wikipedia, Google, and Yahoo!) that contain additional information about the application.
Standard Ports	Ports that the application uses to communicate with the network.
Depends on Applications	List of other applications that are required for this application to run.
Evasive	Indication of whether the application attempts to evade firewalls.
Excessive Bandwidth Use	Indication of whether the application uses too much bandwidth so that network performance may be compromised.
Used by Malware	Indication of whether the application is used by malware.
Capable of File Transfer	Indication of whether the application is able to transfer files.
Has Known Vulnerabilities	Indication of whether the application has any currently known vulnerabilities.
Tunnels Other Applications	Indication of whether the application can carry other applications within the messages that it sends.
Prone to Misuse	Indication of whether the application tends to attract misuse.
Widely used	Indication of whether the effects of the application are wide-ranging.
Category	Application category.
Subcategory	Application sub category.
Technology	Application technology.
Risk	Assigned risk of the application. To customize this setting, click the Customize link, enter a value (1-5), and click OK .
Session Timeout	Period of time (seconds) required for the application to timeout due to inactivity (1-604800 seconds). This timeout is for protocols other than TCP or UDP. For TCP and UDP, see the next rows in this table. To customize this setting, click the Customize link, enter a value (seconds), and click OK .
TCP Timeout (seconds)	Timeout for terminating a TCP application flow (1-604800 seconds). To customize this setting, click the Customize link, enter a value (seconds), and click OK . A value of 0 does not indicate no timeout, it indicates that the global session timer will be used, which is 3600 seconds for TCP.
UDP Timeout (seconds):	Timeout for terminating a UDP application flow (1-604800 seconds). To customize this setting, click the Customize link, enter a value (seconds), and click OK .

Table 156. Application Details (Continued)

Item	Description
TCP Half Closed (seconds)	<p>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.</p> <p>Default: If this timer is not configured at the application level, the global setting is used. Range is 1-604800 sec.</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 that a session remains in the session table after receiving the second FIN or a RST. If the timer expires, the session is closed.</p> <p>Default: If this timer is not configured at the application level, the global setting is used. Range is 1-600 sec</p> <p>If this value is configured at the application level, it overrides the global TCP Time Wait setting.</p>

When the firewall is not able to identify an application using the application 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, see “[Working with Botnet Reports](#)”.

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

Defining Applications

► *Objects > Applications*

Use the **Applications** page to **Add** a new application for the firewall to evaluate when applying policies.

Table 157. New Application Settings

Field	Description
Configuration Tab	
Name	Enter the application name (up to 31 characters). This name appears in the applications list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, periods, hyphens, and underscores. The first character must be a letter.
Shared	<p>Select this check box if you want the application object to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the object will be available only to the vsys selected in the Virtual System drop-down (Objects > Applications page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Application dialog. • All device groups on Panorama. If you clear the check box, the object will be available only to the device group selected in the Device Group drop-down (Objects > Applications page). <p>After you save the object, you cannot change its Shared setting. The Objects > Applications page shows the current setting in the Location field.</p>
Description	Enter a description of the application for general reference (up to 255 characters).
Category	Select the application category, such as email or database. For a description of each category, see “ Application Categories and Subcategories ”. The category is used to generate the Top Ten Application Categories chart and is available for filtering (see “ Using the Application Command Center ”).
Subcategory	Select the application subcategory, such as email or database. For a description of each sub category, see “ Application Categories and Subcategories ”. The sub category is used to generate the Top Ten Application Categories chart and is available for filtering (see “ Using the Application Command Center ”).
Technology	Select the technology for the application. For a description of each technology, see “ Application Technologies ”.
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, see “ Application Characteristics ”.
Advanced Tab	

Table 157. New Application Settings (Continued)

Field	Description
Port	If the protocol used by the application is TCP and/or UDP, select Port and enter one or more combinations of the protocol and port number (one entry per line). The general format is: <i><protocol>/<port></i> where the <i><port></i> is a single port number, or dynamic for dynamic port assignment. Examples: TCP/dynamic or UDP/32. This setting applies when using app-default in the Service column of a security rule.
IP Protocol	To specify an IP protocol other than TCP or UDP, select IP Protocol , and enter the protocol number (1 to 255).
ICMP Type	To specify an Internet Control Message Protocol version 4 (ICMP) type, select ICMP Type and enter the type number (range 0-255).
ICMP6 Type	To specify an Internet Control Message Protocol version 6 (ICMPv6) type, select ICMP6 Type and enter the type number (range 0-255).
None	To specify signatures independent of protocol, select None .
Timeout	Enter the number of seconds before an idle application flow is terminated (range 0-604800 seconds). A zero indicates that the default timeout of the application will be used. This value is used for protocols other than TCP and UDP in all cases and for TCP and UDP timeouts when the TCP timeout and UDP timeout are not specified.
TCP Timeout	Enter the number of seconds before an idle TCP application flow is terminated (range 0-604800 seconds). A zero indicates that the default timeout of the application will be used.
UDP Timeout	Enter the number of seconds before an idle UDP application flow is terminated (range 0-604800 seconds). A zero indicates that the default timeout of the application will be used.
TCP Half Closed	Enter the maximum length of time that a session remains in the session table, between receiving the first FIN and receiving the second FIN or RST. If the timer expires, the session is closed. Default: If this timer is not configured at the application level, the global setting is used. Range is 1-604800 sec. If this value is configured at the application level, it overrides the global TCP Half Closed setting.
TCP Time Wait	Enter the maximum length of time that a session remains in the session table after receiving the second FIN or a RST. If the timer expires, the session is closed. Default: If this timer is not configured at the application level, the global setting is used. Range is 1-600 sec. If this value is configured at the application level, it overrides the global TCP Time Wait setting.
Scanning	Select check boxes for the scanning types that you want to allow, based on security profiles (file types, data patterns, and viruses).

Table 157. New Application Settings (Continued)

Field	Description
Signature Tab	
Signatures	<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 conditions to 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. • Select an operator from Pattern Match and Equal To. When choosing a pattern match operator, specify the following: <ul style="list-style-type: none"> – Context—Select from the available contexts. – Pattern—Specify a regular expression. See Table 162 for pattern rules for regular expressions. – Qualifier and Value—Optionally, add qualifier/value pairs. • When choosing an equal to operator, specify the following, <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, 0xffffffff00. – Value—Specify a 4-byte hex value, for example, 0xaabbccdd. • To move a condition within a group, select the condition and click the Move Up or Move Down arrow. To move a group, select the group and click the Move Up or Move Down arrow. You cannot move conditions from one group to another.



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

To import an application, click **Import**. Browse to select the file, and select the target virtual system from the **Destination** drop-down list.

To export the application, select the check box for the application and click **Export**. Follow the prompts to save the file.

Defining Application Groups

► *Objects > Application Groups*

To simplify the creation of security policies, applications requiring the same security settings can be combined into an application group. (To define a new application, see “[Defining Applications](#)”.)

Table 158. New Application Group

Field	Description
Name	Enter a name that describes the application group (up to 31 characters). This name appears in the application list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	Select this check box if you want the application group object to be available to: <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the object will be available only to the vsys selected in the Virtual System drop-down (Objects > Application Groups page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Application Group dialog. • All device groups on Panorama. If you clear the check box, the object will be available only to the device group selected in the Device Group drop-down (Objects > Application Groups page). After you save the object, you cannot change its Shared setting. The Objects > Application Groups page shows the current setting in the Location field.
Applications	Click Add and select applications, application filters, and/or other application groups to be included in this group.

Application Filters

► *Objects > Application Filters*

You can define application filters to simplify repeated searches. To define application filters to simplify repeated searches, click **Add** and enter a name for the filter.

In the upper area of the window, click an item that you want to use as a basis for filtering. For example, to restrict the list to the Networking category, click **networking**.

Category	Subcategory	Technology	Risk	Characteristic
241 business-systems	31 audio-streaming	476 browser-based	317 1	499 Evasive
333 collaboration	11 auth-service	452 client-server	242 2	394 Excessive Bandwidth
196 general-internet	15 database	197 network-protocol	294 3	264 Prone to Misuse
173 media	56 email	117 peer-to-peer	258 4	612 Transfers Files
299 networking	33 encrypted-tunnel		133 5	249 Tunnels Other Apps
2 unknown	19 erp-crm			266 Used by Malware
	154 file-sharing			733 Vulnerability
	46 gaming			779 Widely used

To filter on additional columns, select an entry in the columns to display check boxes. The

filtering is successive: first category filters are applied, then sub category filters, then technology filters, then risk, filters, and finally characteristic filters.

For example, the next figure shows the result of choosing a category, sub category, and risk filter. In applying the first two filters, the Technology column is automatically restricted to the technologies that are consistent with the selected category and sub category, even though a technology filter has not been explicitly applied.

As you select options, the list of applications in the lower part of the page is automatically updated, as shown in the figure.

Category		Subcategory	Technology	Risk	Characteristic	5 matching applications	
5 collaboration	56 email 91 instant-messaging 30 internet-conferencing	5 browser-based	2 1 1 2 2 3	4 Transfers Files 1 Tunnels Other Apps 4 Vulnerability 2 Widely used			
	5 social-business	64 social-networking 52 voip-video 35 web-posting					
Name	Category	Subcategory		Risk	Technology		
blackboard	collaboration	social-business		1	browser-based		
dearspace	collaboration	social-business		3	browser-based		
projectplace	collaboration	social-business		2	browser-based		
rypple	collaboration	social-business		1	browser-based		
sharepoint (1 out of 6 shown)	collaboration	social-business		3	browser-based		
sharepoint-base							

Services

► Objects > Services

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

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

The following table describes the service settings:

Table 159. Service Settings

Field	Description
Name	Enter the service name (up to 63 characters). This name appears in the services list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the service (up to 255 characters).

Table 159. Service Settings (Continued)

Field	Description
Shared	<p>Select this check box if you want the service object to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the object will be available only to the vsys selected in the Virtual System drop-down (Objects > Services page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Service dialog. • All device groups on Panorama. If you clear the check box, the object will be available only to the device group selected in the Device Group drop-down (Objects > Services page). <p>After you save the object, you cannot change its Shared setting. The Objects > Services page shows the current setting in the Location field.</p>
Protocol	Select the protocol used by the service (TCP or UDP).
Destination Port	Enter the destination port number (0 to 65535) or range of port numbers (port1-port2) used by the service. Multiple ports or ranges must be separated by commas. The destination port is required.
Source Port	Enter the source port number (0 to 65535) or range of port numbers (port1-port2) used by the service. Multiple ports or ranges must be separated by commas. The source port is optional.

Service Groups

► *Objects > Services Groups*

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

The following table describes the service group settings:

Table 160. Service Group Settings

Field	Description
Name	Enter the service group name (up to 63 characters). This name appears in the services list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	<p>Select this check box if you want the service group object to be available to:</p> <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the object will be available only to the vsys selected in the Virtual System drop-down (Objects > Service Groups page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Service Group dialog. All device groups on Panorama. If you clear the check box, the object will be available only to the device group selected in the Device Group drop-down (Objects > Service Groups page). <p>After you save the object, you cannot change its Shared setting. The Objects > Service Groups page shows the current setting in the Location field.</p>
Service	Click Add to add services to the group. Select from the drop-down list, or click the Service button at the bottom of the drop-down list, and specify the settings. See “ Services ” for a description of the settings.

Working with Tags

► *Objects > Tags*

Tags allow you to group objects using keywords or phrases. Tags can be applied to address objects, address groups (static and dynamic), zones, services, service groups, and to policy rules. When tagged, the keyword can be used to sort or filter objects; to visually distinguish objects, you can also apply a color to a tag. When a color is applied to a tag, the **Policy** tab displays the object with the background color.

Use this tab to create, assign a color, delete, rename, and clone tags. Each object can have up to 64 tags; when an object has multiple tags, it takes the color of the first tag in the ordered list of tags applied.

*The **Objects > Tags** tab only displays the tags that you defined locally on the firewall (or on Panorama). If you have configured dynamic address groups, this tab does not display the tags that are dynamically retrieved from the VM Information sources defined on the firewall.*

To add a new tag, click **Add** and then fill in the following fields:

Table 161. Tag Settings

Field	Description
Name	Enter a unique tag name (up to 127 characters). The name is not case-sensitive.
Shared	Select this check box if you want the tag to be available to: <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the tag will be available only to the vsys selected in the Virtual System drop-down (Objects > Tags page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Tag dialog. All device groups on Panorama. If you clear the check box, the tag will be available only to the device group selected in the Device Group drop-down (Objects > Tags page). After you save the tag, you cannot change its Shared setting. The Objects > Tags page shows the current setting in the Location field.
Color	Select a color from the color palette in the drop-down list. The default value is None.
Comments	Add a label or description to remind you what the tag is used for.

Data Patterns

Data pattern support allows you to specify categories of sensitive information that you may want to subject to filtering using data filtering security policies. For instructions on configuring data patterns, see “[Dynamic Block Lists](#)”.

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 is case-sensitive, as with most regular expression engines. Looking for “confidential” is different than looking for “Confidential” or “CONFIDENTIAL.”

The regular expression syntax in PAN-OS is similar to traditional regular expression engines, but every engine is unique. The following table describes the syntax supported in PAN-OS.

Table 162. Pattern Rules

Syntax	Description
.	Match any single character.
?	Match the preceding character or expression 0 or 1 time. The general expression MUST be inside a pair of parentheses. Example: (abc)?
*	Match the preceding character or expression 0 or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)*

Table 162. Pattern Rules

Syntax	Description
+	Match the preceding character or regular expression 1 or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)+
	Equivalent to “or”. Example: ((bif) (scr) (exe)) matches “bif”, “scr” or “exe”. Note that the alternative substrings must be in parentheses.
-	Used to create range expressions. Example: [c-z] matches any character between c and z, inclusive.
[]	Match any. Example: [abz]: matches any of the characters a, b, or z.
^	Match any except. Example: [^abz] matches any character except a, b, or z.
{ }	Min/Max number of bytes. Example: {10-20} matches any string that is between 10 and 20 bytes. This must be directly in front of a fixed string, and only supports “-”.
\	To perform a literal match on any one of the special characters above, it MUST be escaped by preceding them with a ‘\’ (backslash).
&	& 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
 - Does 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”

Dynamic Block Lists

► Objects > Dynamic Block Lists

Use the **Dynamic Block Lists** page to create an address object based on an imported list of IP addresses. The source of the list must be a text file and must be located on a web server. You can set the **Repeat** option to automatically update the list on the device hourly, daily, weekly, or monthly. After creating a dynamic block list object, you can then use the address object in the source and destination fields for security policies.

A maximum of ten dynamic block lists are supported on all platforms. Each list can contain up to 5,000 IP addresses (IPv4 and/or IPv6) that can include IP ranges and/or IP subnets.

The list must contain one IP address, range, or subnet per line, for example:

“192.168.80.150/32” indicates one address, and “192.168.80.0/24” indicates all addresses from 192.168.80.0 through 192.168.80.255.

Example:

“2001:db8:123:1::1” or “2001:db8:123:1::/64”

IP Range:

To specify an address range, select **IP Range**, and enter a range of addresses. The format is:

ip_address–ip_address

where each address can be IPv4 or IPv6.

Example:

“2001:db8:123:1::1 – 2001:db8:123:1::22”

The following table describes the dynamic block list settings:

Table 163 Dynamic Block Lists

Field	Description
Name	Enter a name to identify the Dynamic Block List (up to 32 characters). This name will appear when selecting the source or destination in a policy.
Shared	Select this check box if you want the dynamic block list to be available to: <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the dynamic block list will be available only to the vsys selected in the Virtual System drop-down (Objects > Dynamic Block Lists page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Dynamic Block Lists dialog. All device groups on Panorama. If you clear the check box, the dynamic block list will be available only to the device group selected in the Device Group drop-down (Objects > Dynamic Block Lists page). After you save the dynamic block list, you cannot change its Shared setting. The Objects > Dynamic Block Lists page shows the current setting in the Location field.
Description	Enter a description for the block list (up to 255 characters).
Source	Enter an HTTP or HTTPS URL path that contains the text file. For example, <code>http://1.1.1.1/myfile.txt</code> .
Repeat	Specify the frequency in which the list should be imported. You can choose hourly, daily, weekly, or monthly. At the specified interval, the list will be imported into the configuration. A full commit is not needed for this type of update to occur.
Test Source URL (firewall only)	Test that the source URL or server path is available. This button is only available in the firewall web interface, not in Panorama.

Custom Spyware and Vulnerability Signatures

This section describes the options available to create custom Spyware and Vulnerability signatures that can be used when creating custom vulnerability profiles.

- ▶ *Objects > Custom Objects > Data Patterns*
- ▶ *Objects > Custom Objects > Spyware*
- ▶ *Objects > Custom Objects > Vulnerability*
- ▶ *Objects > Custom Objects > URL Category*

Defining Data Patterns

- *Objects > Custom Objects > Data Patterns*

Use the **Data Patterns** page to define the categories of sensitive information that you may want to subject to filtering using data filtering security policies. For information on defining data filtering profiles, see “[Data Filtering Profiles](#)”.

The following table describes the data pattern settings:

Table 164. Data Pattern Settings

Field	Description
Name	Enter the data pattern name (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the data pattern (up to 255 characters).
Shared	<p>Select this check box if you want the data pattern to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the data pattern will be available only to the vsys selected in the Virtual System drop-down (Objects > Custom Objects > Data Patterns page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Data Patterns dialog. • All device groups on Panorama. If you clear the check box, the data pattern will be available only to the device group selected in the Device Group drop-down (Objects > Custom Objects > Data Patterns page). <p>After you save the data pattern, you cannot change its Shared setting. The Objects > Custom Objects > Data Patterns page shows the current setting in the Location field.</p>
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 0-255). • SSN#—Specify a weight for the social security number field, where the field includes dashes, such as 123-45-6789 (range 0-255, 255 is highest weight). • SSN# (without dash)—Specify a weight for the social security number field, where the entry is made without dashes, such as 123456789 (range 0-255, 255 is highest weight).
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.</p>

Defining Spyware and Vulnerability Signatures

- *Objects > Custom Objects > Spyware*
- *Objects > Custom Objects > Vulnerability*

The firewall supports the ability to create custom spyware and vulnerability signatures using

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



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

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

Use the **Custom Spyware Signature** page to define signatures for anti-spyware profiles. Use the **Custom Vulnerability Signature** page to define signatures for vulnerability protection profiles.

Table 165. Custom Signatures - Vulnerability and Spyware

Field	Description
Configuration Tab	
Threat ID	Enter a numeric identifier for the configuration. For spyware signatures, the range is 15000-18000; for vulnerability signatures the range is 41000-45000.
Name	Specify the threat name.
Shared	<p>Select this check box if you want the custom signature to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the signature will be available only to the vsys selected in the Virtual System drop-down (Objects > Custom Objects > Spyware/Vulnerability page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Custom Spyware/Vulnerability Signature dialog. • All device groups on Panorama. If you clear the check box, the signature will be available only to the device group selected in the Device Group drop-down (Objects > Custom Objects > Spyware/Vulnerability page). <p>After you save the signature, you cannot change its Shared setting. The Objects > Custom Objects > Spyware/Vulnerability page shows the current setting in the Location field.</p>
Comment	Enter an optional comment.
Severity	Assign a level that indicates the seriousness of the threat.
Default Action	<p>Assign the default action to take if the threat conditions are met:</p> <ul style="list-style-type: none"> • Alert—Generate an alert. • Drop Packets—Do not allow packets through. • Reset Both—Reset the client and server. • Reset Client—Reset the client. • Reset Server—Reset the server. • Block IP—Block traffic for a specified period of time. Choose whether to block traffic for the source only or source and destination, and enter the duration (seconds).
Direction	Indicate whether the threat is assessed from the client to server, server to client, or both.
Affected System	Indicate whether the threat involves the client, server, either, or both. Applies to vulnerability signatures, but not spyware signatures.
CVE	Specify the common vulnerability enumeration (CVE) as an external reference for additional background and analysis.
Vendor	Specify the vendor identifier for the vulnerability as an external reference for additional background and analysis.
Bugtraq	Specify the bugtraq (similar to CVE) as an external reference for additional background and analysis.

Table 165. Custom Signatures - Vulnerability and Spyware (Continued)

Field	Description
Reference	Add any links to additional analysis or background information. The information is shown when a user clicks on the threat from the ACC, logs, or vulnerability profile.
Signatures Tab	
Standard Signature	<p>Select the Standard radio button and then click Add to 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>Specify conditions to 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. Select from the Method and Context drop-down lists. Specify a regular expression in the Pattern field. Add additional patterns as needed. • To move a condition within a group, select the condition and click the Move Up or Move Down arrow. To move a group, select the group and click the Move Up or Move Down arrow. You cannot move conditions from one group to another.
Combination Signature	<p>Select the Combination radio button. In the area above the subtabs, specify the following information:</p> <p>On the Combination Signatures subtab, specify conditions to 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. Select from the Method and Context drop-down lists. Specify a regular expression in the Pattern field. Add additional patterns as needed. • To move a condition within a group, select the condition and click the Move Up or Move Down arrow. To move a group, select the group and click the Move Up or Move Down arrow. You cannot move conditions from one group to another. <p>On the Time Attribute subtab, 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.

Custom URL Categories

► *Objects > Custom Objects > URL Category*

The custom URL categories feature allows you to create your own lists of URLs that can be selected in any URL filtering profile. Each custom category can be controlled independently

and will have an action associated with it in each URL filtering profile (allow, block, continue, override, alert, or none). The *none* action only applies to custom URL categories. The purpose of selecting *none* is to ensure that if multiple URL profiles exist, the custom category will not have any impact on other profiles. For example, if you have two URL profiles and the custom URL category is set to block in one of the profiles, the other profile should have the action set to *none* if you do not want it to apply.

URL entries can be added individually, or you can import a list of URLs. To do so, create a text file that contains the URLs to include, with one URL per line. Each URL can be in the format “www.example.com,” and can contain * as a wildcard, such as “*.example.com.” For additional information on wildcards, see the description of Block List in Table 147 on page 246.



URL entries added to custom categories are case insensitive. Also, to delete a custom category after it has been added to a URL profile and an action has been set, the action must be set to None before the custom category can be deleted.

For instructions on setting up URL filtering profiles, see “[URL Filtering Profiles](#)”.

The following table describes the custom URL settings:

Table 166. Custom URL Categories

Field	Description
Name	Enter a name to identify the custom URL category (up to 31 characters). This name appears in the category list when defining URL filtering policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the URL category (up to 255 characters).
Shared	Select this check box if you want the custom URL category to be available to: <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the category will be available only to the vsys selected in the Virtual System drop-down (Objects > Custom Objects > URL Category page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Custom URL Category dialog. All device groups on Panorama. If you clear the check box, the category will be available only to the device group selected in the Device Group drop-down (Objects > Custom Objects > URL Category page). After you save the URL category, you cannot change its Shared setting. The Objects > Custom Objects > URL Category page shows the current setting in the Location field.
Sites	In the Sites area, click Add to enter a URL or click Import and browse to select the text file that contains the list of URLs.

Security Profile Groups

► *Objects > Security Profile Groups*

The firewall supports the ability to create security profile groups, which specify sets of security profiles that can be treated as a unit and then added to security policies. For example, you can create a “threats” security profile group that includes profiles for antivirus, anti-spyware, and vulnerability and then create a security policy that includes the “threats” profile.

Antivirus, anti-spyware, vulnerability protection, URL filtering, and file blocking profiles that are often assigned together can be combined into profile groups to simplify the creation of security policies.

To define new security profiles, see “[Defining Security Policies](#)”.

The following table describes the security profile settings:

Table 167. Security Profile Group Settings

Field	Description
Name	<p>Enter a descriptive name for a security profile group or enable a default security profile group:</p> <ul style="list-style-type: none"> 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. Create a new security profile group or modify an existing profile group to be used as the default security profile settings for new security policies. Name a security profile group <i>default</i> to enable it to be automatically included in new security policies.
Shared	<p>Select this check box if you want the security profile group to be available to:</p> <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the group will be available only to the vsys selected in the Virtual System drop-down (Objects > Security Profile Group page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Security Profile Group dialog. All device groups on Panorama. If you clear the check box, the group will be available only to the device group selected in the Device Group drop-down (Objects > Security Profile Group page). <p>After you save the security profile group, you cannot change its Shared setting. The Objects > Security Profile Group page shows the current setting in the Location field.</p>
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. See “ Data Filtering Profiles ”.

Log Forwarding

► *Objects > Log Forwarding*

Each security policy can specify a log forwarding profile that determines whether traffic and threat log entries are logged remotely with Panorama, and/or sent as SNMP traps, syslog messages, or email notifications. By default, only local logging is performed.

Traffic logs record information about each traffic flow, and threat logs record the threats or problems with the network traffic, such as virus or spyware detection. Note that the antivirus, anti-spyware, and vulnerability protection profiles associated with each rule determine which threats are logged (locally or remotely). To apply logging profiles to security policies, see “[Defining Security Policies](#)”.



On a PA-7050 firewall, a special interface type (Log Card) must be configured before the firewall will forward the following log types: Syslog, Email, and SNMP. This is also required to forward files to WildFire. After the port is configured, log forwarding and WildFire forwarding will automatically use this port and there is no special configuration required for this to occur. Just configure a data port on one of the PA-7050 NPCs as interface type Log Card and ensure that the network that will be used can communicate with your log servers. For WildFire forwarding, the network will need to communicate with the WildFire cloud and/or WildFire appliance. For information on configuring this interface, see “Configuring a Log Card Interface”.

A PA-7050 firewall 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-7050 firewall, Panorama queries the firewall in real-time to display its log data.

The following table describes the log forwarding settings:

Table 168. Log Forwarding Profile Settings

Field	Description
Name	<p>Enter a descriptive name for a log forwarding profile or enable a default log forwarding profile:</p> <ul style="list-style-type: none"> 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. Create a new log forwarding profile or modify an existing log forwarding profile to be used as the default log forwarding settings for new security policies and new security zones. Name the log forwarding profile <i>default</i> to enable it to be used as the default log forwarding profile.
Shared	<p>Select this check box if you want the log forwarding profile to be available to:</p> <ul style="list-style-type: none"> All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the Virtual System drop-down (Objects > Log Forwarding page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Log Forwarding Profile dialog. All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the Device Group drop-down (Objects > Log Forwarding page). <p>After you save the profile, you cannot change its Shared setting. The Objects > Log Forwarding page shows the current setting in the Location field.</p>
Traffic Settings	
Panorama	Select the check box to enable sending traffic log entries to the Panorama centralized management system. To define the Panorama server address, see “ Defining Management Settings ”.
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, see:</p> <ul style="list-style-type: none"> “Configuring SNMP Trap Destinations”. “Custom Syslog Field Descriptions” “Configuring Syslog Servers”

Table 168. Log Forwarding Profile Settings (Continued)

Field	Description
Threat Log Settings	
Panorama	<p>Click the check box 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, including URL blocking. • Low—Warning-level attacks detected by the threat security engine. • Informational—All other events not covered by the other severity levels, including informational attack object matches.
SNMP Trap Email Syslog	Under each severity level, select the SNMP, syslog, and/or email settings that specify additional destinations where the threat log entries are sent.

Decryption Profiles

► Objects > Decryption Profile

Decryption profiles enable you to block and control specific aspects of the SSL forward proxy, SSL inbound inspection, and SSH traffic. After you create a decryption profile, you can then apply that profile to a decryption policy.



Before you can enable decryption port mirroring, you must obtain a Decryption Port Mirror license, install the license, and reboot the firewall.

You can also control the trusted CAs that your device trusts, for more information, see “[Managing the Default Trusted Certificate Authorities](#)”.

The following table describes the decryption profile settings:

Table 169. Decryption Profile Settings

Field	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of decryption profiles when defining decryption policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	<p>Select this check box if you want the decryption profile to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the Virtual System drop-down (Objects > Decryption Profile page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Decryption Profile dialog. • All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the Device Group drop-down (Objects > Decryption Profile page). <p>After you save the profile, you cannot change its Shared setting. The Objects > Decryption Profile page shows the current setting in the Location field.</p>

Table 169. Decryption Profile Settings (Continued)

Field	Description
Interface	Select an interface to use for decryption port mirroring.
Forwarded Only	Select this check box if you want to mirror decrypted traffic only after security policy enforcement. With this option, only traffic that is forwarded through the firewall is mirrored. This option is useful if you are forwarding the decrypted traffic to other threat detection devices, such as a DLP device or another intrusion prevention system (IPS). If you clear the check box (the default setting), the firewall will mirror all decrypted traffic to the interface before security policies lookup, which allows you to replay events and analyze traffic that generates a threat or triggers a drop action.
SSL Forward Proxy Tab	
Server Certificate Checks	Select options to control server certificates.
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.
Restrict certificate extensions	<p>Limits the certificate extensions used in the dynamic server certificate to key usage and extended key usage.</p> <p>Details—Displays details on the values used for key usage and extended key usage.</p>
Unsupported Mode Checks	Select options to control unsupported SSL applications.
Block sessions with unsupported version	Terminate sessions if the “client hello” message is not supported by PAN-OS. The SSL versions supported by PAN-OS are: SSLv3, TLS1.0, TLS1.1, and TLS1.2.
Block sessions with unsupported cipher suites	Terminate the session if the cipher suite specified in the SSL handshake if it is not supported by PAN-OS.
Block sessions with client authentication	Terminate sessions with client authentication for SSL forward proxy traffic.
Failure Checks	Select the action to take if system resources are not available to process decryption.
Block sessions if resources not available	Terminate sessions if system resources are not available to process decryption.
Block sessions if HSM not available	Terminate sessions if a hardware security module (HSM) is not available to sign certificates.
<p><i>Note:</i> For unsupported modes and failure modes, the session information is cached for 12 hours, so future sessions between the same hosts and server pair are not decrypted. Use the check boxes to block those sessions instead.</p>	
SSL Inbound Inspection Tab	

Table 169. Decryption Profile Settings (Continued)

Field	Description
Unsupported Mode Checks	Selection options to control sessions if unsupported modes are detected in SSL traffic.
Block sessions with unsupported versions	Terminate sessions if the “client hello” message is not supported by PAN-OS. The SSL versions supported by PAN-OS are: 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.
SSH Tab	
Unsupported Mode Checks	Selection options to control sessions if unsupported modes are detected in SSH traffic. Supported SSH version is SSH version 2.
Block sessions with unsupported versions	Terminate sessions if the “client hello” message is not supported by PAN-OS.
Block sessions with unsupported algorithms	Terminate sessions if the algorithm specified by the client or server is not supported by PAN-OS.
Failure Checks	Select actions to take if SSH application errors occur and if system resources are not available.
Block sessions on SSH errors	Terminate sessions if SSH errors occur.
Block sessions if resources not available	Terminate sessions if system resources are not available to process decryption.

Schedules

► *Objects > Schedules*

By default, each security policy applies to all dates and times. To limit a security policy to specific times, you can define schedules, and then apply them to the appropriate policies. For each schedule, you can specify a fixed date and time range or a recurring daily or weekly schedule. To apply schedules to security policies, see “[Defining Security Policies](#)”.



When a security policy is invoked by a defined schedule, only new sessions are affected by the applied security policy. Existing sessions are not affected by the scheduled policy.

The following table describes the schedule settings:

Table 170. Schedule Settings

Field	Description
Name	Enter a schedule name (up to 31 characters). This name appears in the schedule list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	<p>Select this check box if you want the schedule to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the schedule will be available only to the vsys selected in the Virtual System drop-down (Objects > Schedules page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the Schedule dialog. • All device groups on Panorama. If you clear the check box, the schedule will be available only to the device group selected in the Device Group drop-down (Objects > Schedules page). <p>After you save the schedule, you cannot change its Shared setting. The Objects > Schedules page shows the current setting in the Location field.</p>
Recurrence	Select the type of schedule (Daily , Weekly , or Non-Recurring).
Daily	Click Add and specify a start and end time in 24-hour format (HH:MM).
Weekly	Click Add , select a day of the week, and specify the start and end time in 24-hour format (HH:MM).
Non-recurring	Click Add and specify a start and end date and time.

Chapter 6

Reports and Logs

This section describes how to view the reports and logs provided with the firewall:

- [“Using the Dashboard”](#)
- [“Using the Application Command Center”](#)
- [“Using App Scope”](#)
- [“Viewing the Logs”](#)
- [“Working with Botnet Reports”](#)
- [“Managing PDF Summary Reports”](#)
- [“Managing User/Group Activity Reports”](#)
- [“Managing Report Groups”](#)
- [“Scheduling Reports for Email Delivery”](#)
- [“Viewing Reports”](#)
- [“Generating Custom Reports”](#)
- [“Taking Packet Captures”](#)
- [“Taking Packet Captures”](#)



Most of the reports in this section support optional selection of a virtual system from the drop-down list at the top of page.

Using the Dashboard

► Dashboard

The **Dashboard** page Widgets show general device information, such as the software version, the operational status of each interface, resource utilization, and up to 10 entries in the threat, configuration, and system logs. Log entries from the last 60 minutes are displayed. All of the available Widgets are displayed by default, but each user can remove and add individual Widgets, as needed.

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

Table 171. Dashboard Charts

Chart	Description
Top Applications	Displays the applications with the most sessions. The block size indicates the relative number of sessions (mouse-over the block to view the number), and the color indicates the security risk—from green (lowest) to red (highest). Click an application to view its application profile.
Top High Risk Applications	Similar to Top Applications, except that it displays the highest-risk applications with the most sessions.
General Information	Displays the device name, model, PAN-OS software version, the application, threat, and URL filtering definition versions, the current date and time, and the length of time since the last restart.
Interface Status	Indicates whether each interface is up (green), down (red), or in an unknown state (gray).
Threat Logs	Displays the threat ID, application, and date and time for the last 10 entries in the Threat log. The threat ID is a malware description or URL that violates the URL filtering profile. Only entries from last 60 minutes are displayed.
Config Logs	Displays the administrator user name, client (Web or CLI), and date and time for the last 10 entries in the Configuration log. Only entries from the last 60 minutes are displayed.
Data Filtering Logs	Displays the description and date and time for the last 60 minutes in the Data Filtering log.
URL Filtering Logs	Displays the description and date and time for the last 60 minutes in the URL Filtering log.
System Logs	Displays the description and date and time for the last 10 entries in the System log. Note that a “Config installed” entry indicates configuration changes were committed successfully. Only entries from the last 60 minutes are displayed.

Table 171. Dashboard Charts (Continued)

Chart	Description
System Resources	Displays the Management CPU usage, Data Plane usage, and the Session Count, which displays the number of sessions established through the firewall.
Logged In Admins	Displays the source IP address, session type (Web or CLI), and session start time for each administrator who is currently logged in.
ACC Risk Factor	Displays the average risk factor (1 to 5) for the network traffic processed over the past week. Higher values indicate higher risk.
High Availability	If high availability (HA) is enabled, indicates the HA status of the local and peer device—green (active), yellow (passive), or black (other). For more information about HA, see “ Enabling HA on the Firewall ”.
Locks	Shows configuration locks taken by administrators.

Using the Application Command Center

► ACC

There are 5 charts displayed on the **Application Command Center (ACC)** page:

- [“Application”](#)
- [“URL Filtering”](#)
- [“Threat Prevention”](#)
- [“Data Filtering”](#)
- [“HIP Matches”](#)

The Application Command Center (ACC) page visually depicts trends and historic view of traffic on your network. It displays the overall risk level for all network traffic, the risk levels and number of threats detected for the most active and highest-risk applications on your network, and the number of threats detected from the busiest application categories and from all applications at each risk level. The ACC can be viewed for the past hour, day, week, month, or any custom-defined time frame.

Risk levels (1=lowest to 5=highest) indicate the application’s relative security risk based on criteria such as whether the application can share files, is prone to misuse, or tries to evade firewalls.

To view the Application Command Center:

1. Under the **ACC** tab, change one or more of the following settings at the top of the page:
 - a. Select a virtual system, if virtual systems are defined.
 - b. Select a time period from the **Time** drop-down list. The default is Last Hour.
 - c. Select a sorting method from the **Sort By** drop-down list. You can sort the charts in descending order by number of sessions, bytes, or threats. The default is by number of sessions.

- d. For the selected sorting method, select the top number of applications and application categories shown in each chart from the **Top** drop-down list.
- e. (Only for Panorama) Select the **Data Source** that is used to generate the graphical display on traffic trends.

Click the submit icon  to apply the selected settings.

The default **Data Source** for new installations is Panorama; Panorama uses the logs forwarded by the managed devices. To fetch and display an aggregated view of the data from the managed devices, you now have to switch the source from **Panorama** to **Remote Device Data**. On an upgrade, the default data source is **Remote Device Data**.

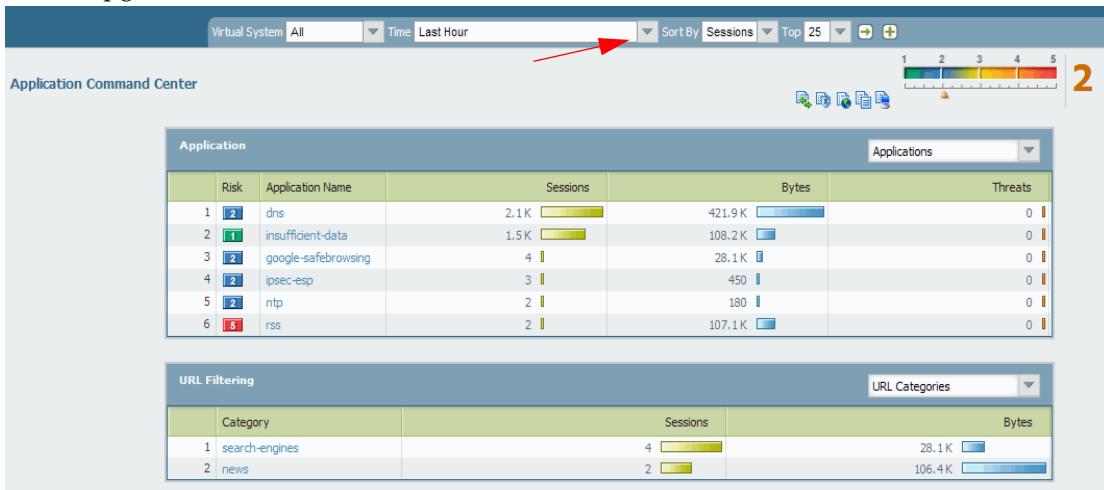


Figure 5. Application Command Center Page

2. To open log pages associated with the information on the page, use the log links in the upper-right corner of the page, as shown here. The context for the logs matches the information on the page.



3. To filter the list, click an item in one of the columns, this will add that item to the filter bar located above the log column names. After adding the desired filters, click the Apply Filter icon .



The screenshot shows a log search results table. The header row includes a search bar with the query '(receive_time in last-hour) and (zone.src eq l3-vlan-trust) and (addr.src in 192.168.2.10)' and various filter and search icons. The table has columns: Receive Time, Type, From Zone, To Zone, Source, Source User, and Destination. There are two rows of data:

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
	09/05 16:44:14	end	l3-vlan-trust	l3-untrust	192.168.2.10		10.0.1
	09/05 16:44:14	end	l3-vlan-trust	l3-untrust	192.168.2.10		10.0.1

4. Choose a view from the drop-down list for the area of interest, as described in the following table.
5. Use the drop-down lists for Applications, URL Categories, Threats, Content/File Types, and HIP Objects.

Table 172. Application Command Center Charts

Chart	Description
Application	<p>Displays information organized according to the menu selection. Information includes the number of sessions, bytes transmitted and received, number of threats, application category, application subcategories, application technology, and risk level, as applicable.</p> <ul style="list-style-type: none"> • Applications • High risk applications • Categories • Sub Categories • Technology • Risk
URL Filtering	<p>Displays information organized according to the menu selection. Information includes the URL, URL category, repeat count (number of times access was attempted, as applicable).</p> <ul style="list-style-type: none"> • URL Categories • URLs • Blocked URL Categories • Blocked URLs
Threat Prevention	<p>Displays information organized according to the menu selection. Information includes threat ID, count (number of occurrences), number of sessions, and subtype (such as vulnerability), as applicable.</p> <ul style="list-style-type: none"> • Threats • Types • Spyware • Spyware Phone Home • Spyware Downloads • Vulnerability • Virus
Data Filtering	<ul style="list-style-type: none"> • Content/File Types • Types • File Names
HIP Matches	<ul style="list-style-type: none"> • HIP Objects • HIP Profiles

6. To view additional details, click any of the links. A details page opens to show information about the item at the top and additional lists for related items.

Application Information

Name: web-browsing	Category: general-internet
Description: Web Browsing is using Hypertext Transfer Protocol (HTTP), which is a method used to transfer or convey information on the World Wide Web. Its original purpose was to provide a way to publish and retrieve HTML pages.	Subcategory: internet-utility
Standard Ports: tcp/80	Technology: browser-based
Capable of File Transfer: yes	Risk: 4
Used by Malware: yes	Widely Used: yes
Excessive Bandwidth Use: no	Has Known Vulnerabilities: yes
Evasive: no	Prone to Misuse: no
Tunnels Other Applications: yes	Session Timeout (seconds):
Additional Information: Wikipedia Google Yahoo!	TCP Timeout (seconds):
	UDP Timeout (seconds):

Top Applications

	Risk	Application	Sessions	Bytes
1	4	web-browsing	559	11.1 M

Top Sources

	Source address	Source Host Name	Source User	Bytes	Sessions
1	10.16.0.54	10.16.0.54		9.9 M	491
2	10.16.1.1	10.16.1.1		829.3 K	45
3	10.16.0.33	10.16.0.33		220.2 K	13
4	10.16.0.34	10.16.0.34		25.0 K	7
5	10.16.0.34	10.16.0.34	paloaltonetwork\jpara...	121.4 K	3

Figure 6. Application Command Center Drill Down Page

Using App Scope

► *Monitor > App Scope*

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

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

With the App Scope reports, you can quickly see if any behavior is unusual or unexpected, and helps pinpoint problematic behavior; each report provides a dynamic, user-customizable window into the network. The reports include options to select the data and ranges to display. On Panorama, you can also select the **Data Source** for the information that is displayed. The default data source (on new Panorama installations) uses the local database on Panorama, that stores logs forwarded by the managed devices; on an upgrade the default data source is the remote device data. To fetch and display an aggregated view of the data directly from the managed devices, you now have to switch the source from **Panorama** to **Remote Device Data**. Hovering the mouse over and clicking either the lines or bars on the charts switches to the ACC and provides detailed information about the specific application, application category, user, or source.

Table 173. Application Command Center Charts

Chart	Description
Summary	“Summary Report”
Change Monitor	“Change Monitor Report”
Threat Monitor	“Threat Monitor Report”
Threat Map	“Threat Map Report”
Network Monitor	“Network Monitor Report”
Traffic Map	“Traffic Map Report”

Summary Report

The Summary report (Figure 7) displays charts for the top five gainers, losers, and bandwidth consuming applications, application categories, users, and sources.

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

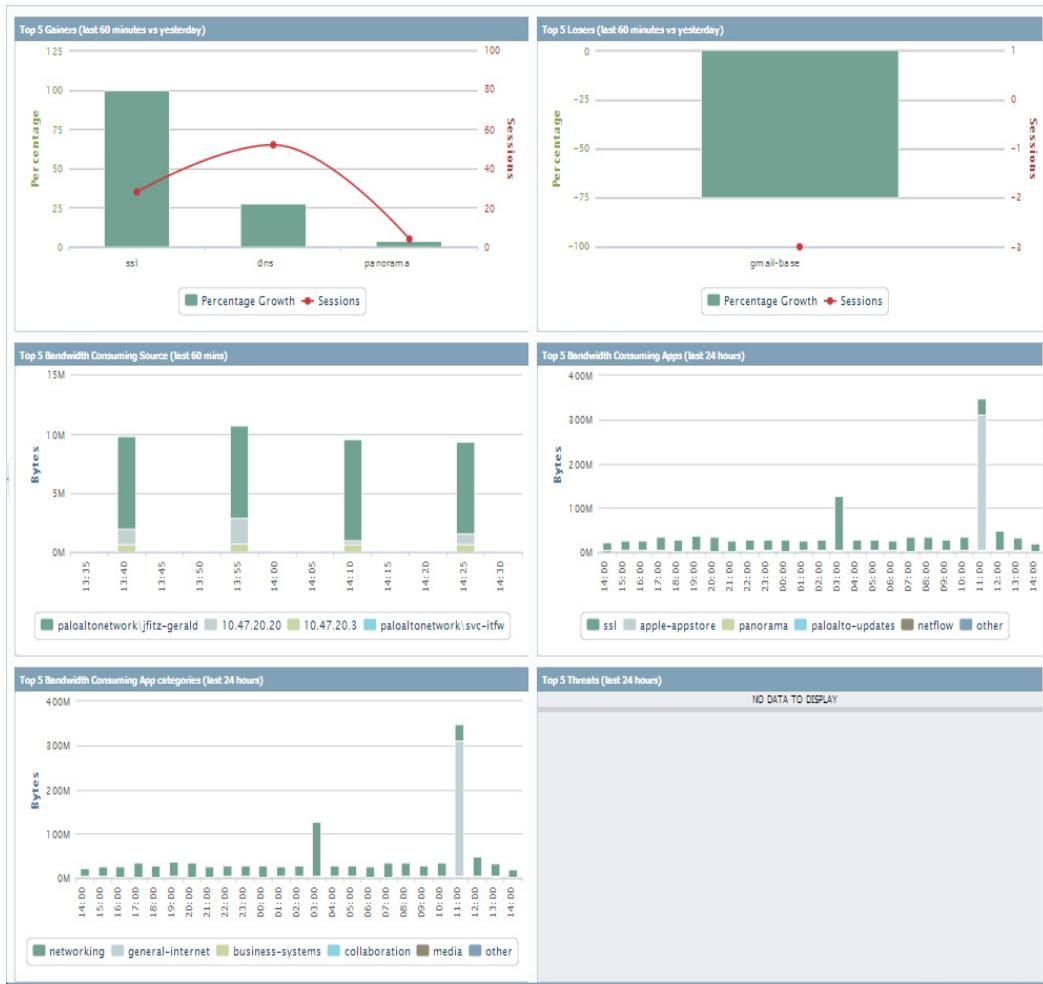


Figure 7. App Scope Summary Report

Change Monitor Report

The Change Monitor report (Figure 8) displays changes over a specified time period. For example, Figure 8 displays the top applications that gained in use over the last hour as compared with the last 24-hour period. The top applications are determined by session count and sorted by percentage.

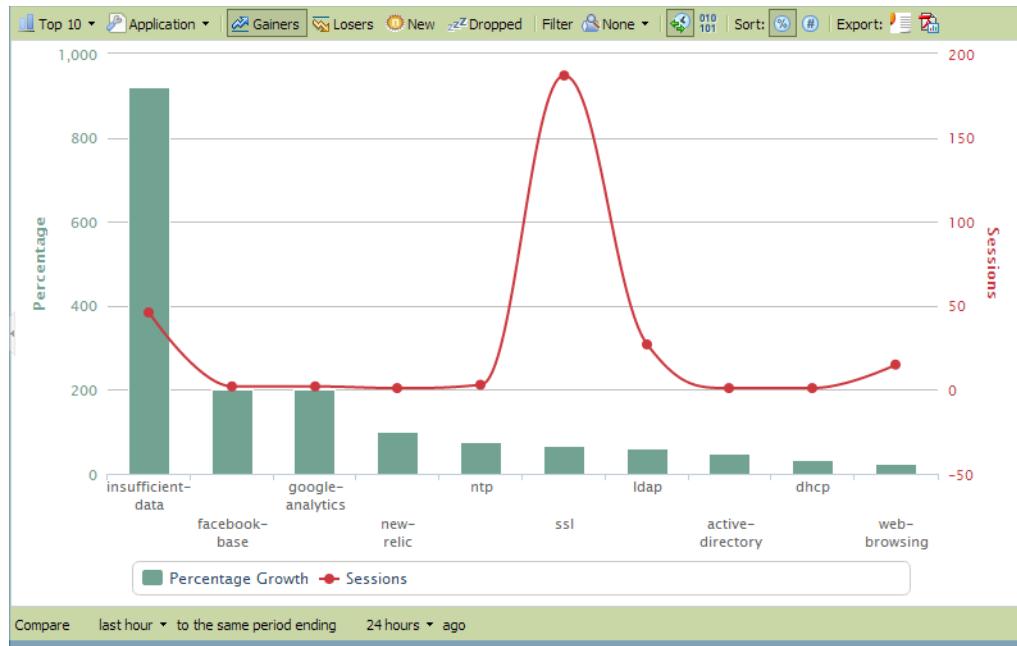
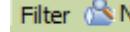


Figure 8. App Scope Change Monitor Report

This report contains the following buttons and options.

Table 174. Change Monitor Report Options

Item	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.
 010 101	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  last hour ▾ to the same period ending  24 hours ▾ ago	Specifies the period over which the change measurements are taken.

Threat Monitor Report

The Threat Monitor report (Figure 9) displays a count of the top threats over the selected time period. For example, Figure 9 shows the top 10 threat types for the past 6 hours.

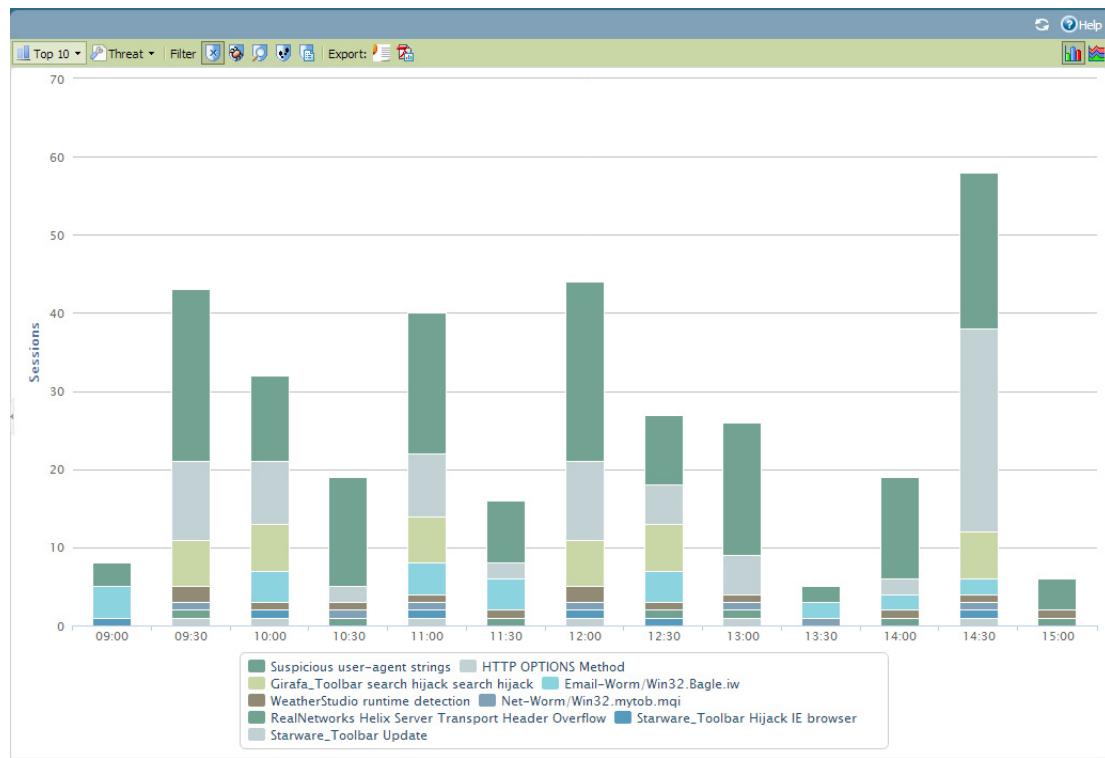
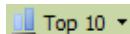
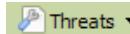


Figure 9. App Scope Threat Monitor Report

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

Table 175. Threat Monitor Report Buttons

Button	Description
Top Bar	
 Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
 Threats ▾	Determines the type of item measured: Threat, Threat Category, Source, or Destination.
 Filter     	Applies a filter to display only the selected type of items.
  	Determines whether the information is presented in a stacked column chart or a stacked area chart.
 Export:  	Exports the graph as a .png image or as a PDF.
Bottom Bar	
Last 6 hours  Last 12 hours  Last 24 hours  Last 7 days  Last 30 days 	Specifies the period over which the measurements are taken.

Threat Map Report

The Threat Map report (Figure 10) shows a geographical view of threats, including severity.

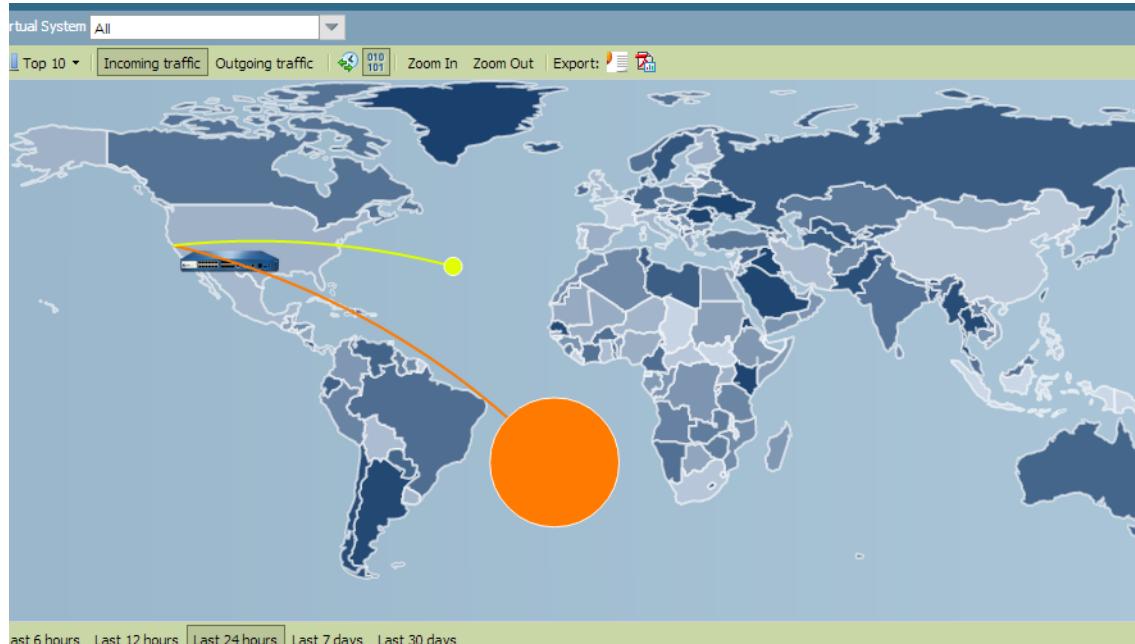
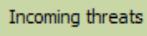
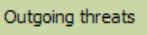
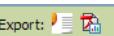


Figure 10. App Scope Threat Map Report

Each threat type is color-coded as indicated in the legend below the chart. Click a country on the map to zoom in. Click the **Zoom Out** button in the lower right corner of the screen to zoom out. This report contains the following buttons and options.

Table 176. Threat Map Report Buttons

Button	Description
Top Bar	
 Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
 Incoming threats	Displays incoming threats.
 Outgoing threats	Displays outgoing threats.
 Filter	Applies a filter to display only the selected type of items.
 Zoom In Zoom Out	Zoom in and zoom out of the map.
 Export:  	Exports the graph as a .png image or as a PDF.
Bottom Bar	
 Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indicates the period over which the measurements are taken.

Network Monitor Report

The Network Monitor report (Figure 11) displays the bandwidth dedicated to different network functions over the specified period of time. Each network function is color-coded as indicated in the legend below the chart. For example, Figure 11 shows application bandwidth for the past 7 days based on session information.

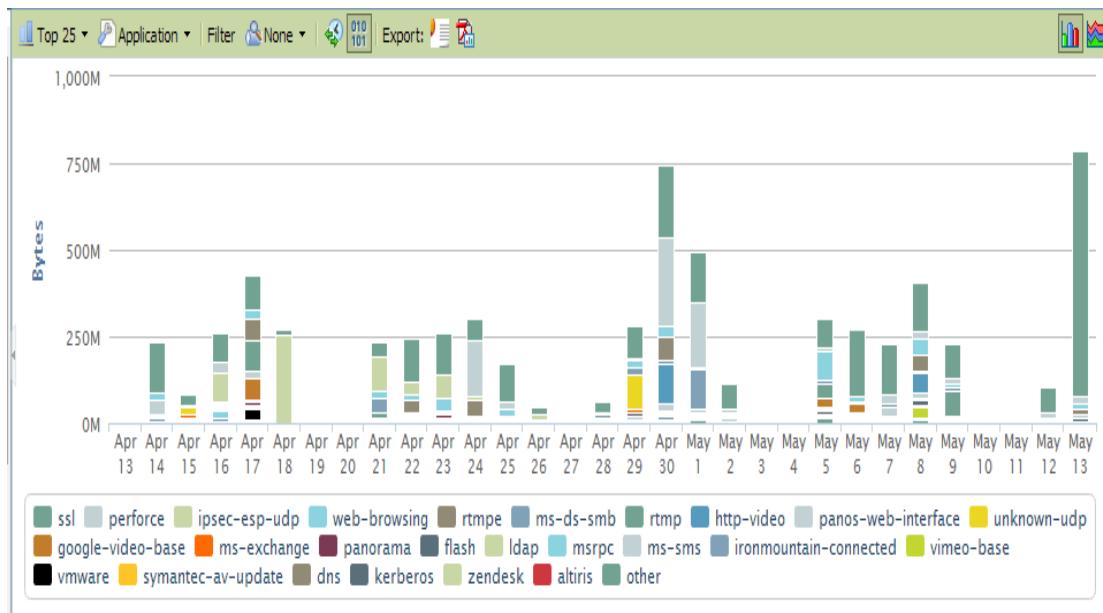


Figure 11. App Scope Network Monitor Report

The report contains the following buttons and options.

Table 177. Network Monitor Report Buttons

Button	Description
Top Bar	
Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
Application ▾	Determines the type of item reported: Application, Application Category, Source, or Destination.
Filter None ▾	Applies a filter to display only the selected item. None displays all entries.
	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	Indicates the period over which the change measurements are taken.
Last 12 hours	
Last 24 hours	
Last 7 days	
Last 30 days	

Traffic Map Report

The Traffic Map report (Figure 12) shows a geographical view of traffic flows according to sessions or flows.

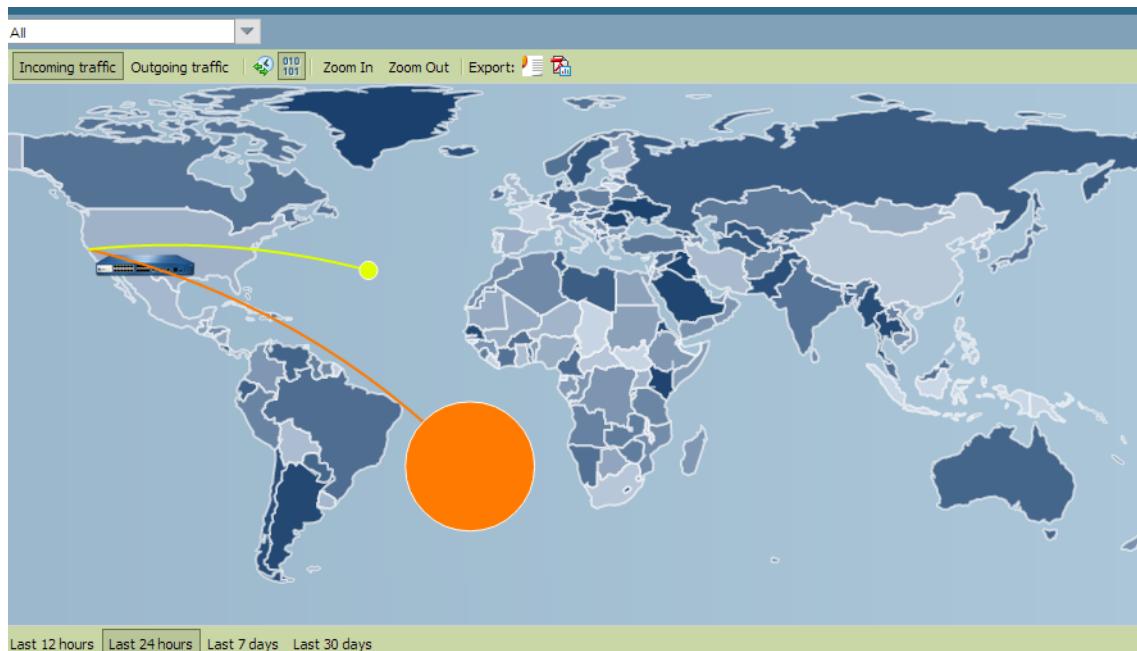
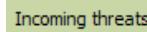
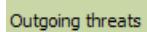
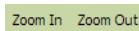


Figure 12. App Scope Traffic Map Report

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

Table 178. Threat Map Report Buttons

Button	Description
Top Bar	
 Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
 Incoming threats	Displays incoming threats.
 Outgoing threats	Displays outgoing threats.
	Determines whether to display session or byte information.
 Zoom In Zoom Out	Zoom in and zoom out of the map.
 Export:  	Exports the graph as a .png image or as a PDF.
Bottom Bar	
 Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indicates the period over which the change measurements are taken.

Viewing the Logs

► *Monitor > Logs*

The firewall maintains logs for WildFire, configurations, system, alarms, traffic flows, threats, URL filtering, data filtering, and Host Information Profile (HIP) matches. You can view the current logs at any time. To locate specific entries, you can apply filters to most of the log fields.



The firewall displays the information in logs so that role-based administration permissions are respected. When you display logs, only the information that you have permission to see is included. For information on administrator permissions, see “Defining Administrator Roles”.

To view the logs, click the log types on the left side of the page in the **Monitor** tab. Each log page has a filter area at the top of the page.



Use the filter area as follows:

- Click any of the underlined links in the log listing to add that item as a log filter option. For example, if you click the **Host** link in the log entry for 10.0.0.252 and **Web Browsing** in both items are added, and the search will find entries that match both (AND search).

- To define other search criteria, click the **Add Log Filter** icon. Select the type of search (and/or), the attribute to include in the search, the matching operator, and the values for the match, if appropriate. Click **Add** to add the criterion to the filter area on the log page, and then click **Close** to close the pop-up window. Click the **Apply Filter** icon to display the filtered list.



If the **Value** string matches an **Operator** (such as **has** or **in**), enclose the string in quotation marks to avoid a syntax error. For example, if you filter by destination country and use **IN** as a **Value** to specify INDIA, enter the filter as (`dstloc eq "IN"`).

You can combine filter expressions added on the log page with those you define in the Add Log Filter dialog. The filter field on the log page displays each filter as an entry.

If you add a **Receive Time** filter with the **Operator** set to **in** and the **Value** set to **Last 60 seconds**, some of the page links on the log viewer might not show results because the number of pages might grow or shrink due to the dynamic nature of the selected time.

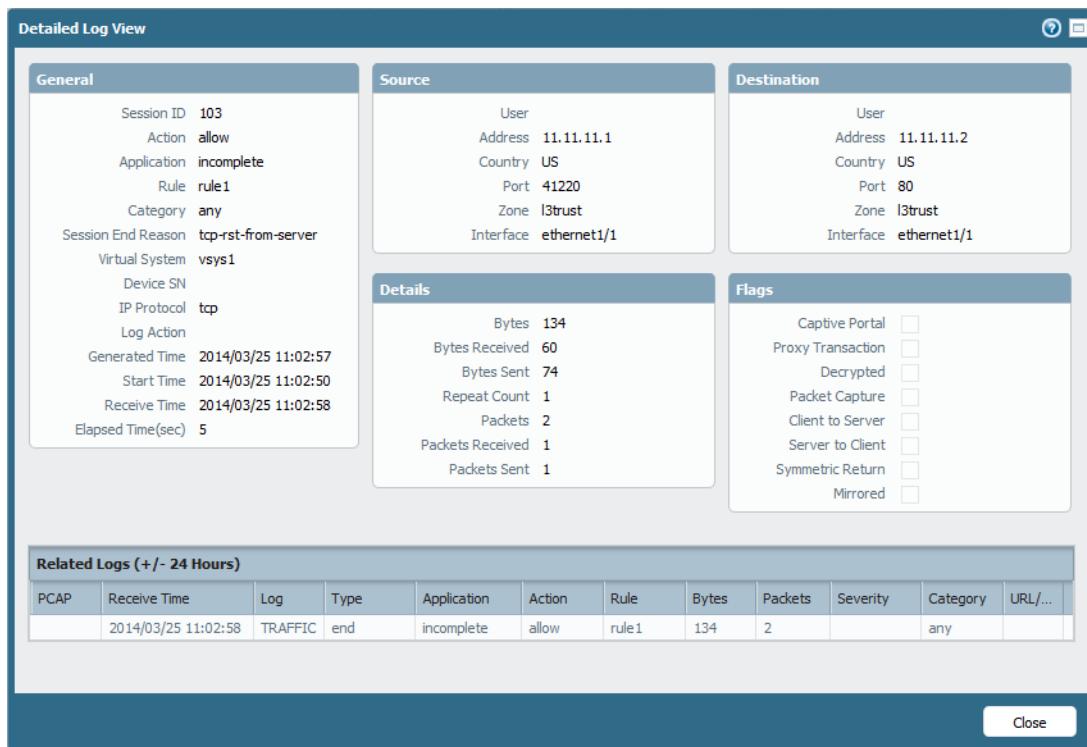
- To clear filters and redisplay the unfiltered list, click the **Clear Filter** button.
- To save your selections as a new filter, click the **Save Filter** button, enter a name for the filter, and click **OK**.
- To export the current log listing (as shown on the page, including any applied filters) click the **Save Filter** button. Select whether to open the file or save it to disk, and select the check box if you want to always use the same option. Click **OK**.
- To export the current log listing in CSV format, select the Export to CSV icon . By default, exporting the log listing to CSV format will generate a CSV report with up to 2,000 lines of logs. To change the line limit for generated CSV reports, use the **Max Rows in CSV Export** field (select **Device > Setup > Management > Logging and Reporting Settings > Log Export and Reporting** or see “[Defining Management Settings](#)”).

To change the automatic refresh interval, select an interval from the drop-down list (1 min, 30 seconds, 10 seconds, or Manual). To change the number of log entries per page, select the number of rows from the **Rows** drop-down list.

Log entries are retrieved in blocks of 10 pages. Use the paging controls at the bottom of the page to navigate through the log list. Select the **Resolve Hostname** check box to begin resolving external IP addresses to domain names.

Select the Export to CSV icon to export a log in CSV format.

To display additional details, click the spyglass icon  for an entry.



The screenshot shows the 'Detailed Log View' window with the following sections:

- General:**
 - Session ID: 103
 - Action: allow
 - Application: incomplete
 - Rule: rule1
 - Category: any
 - Session End Reason: tcp-rst-from-server
 - Virtual System: vsys1
 - Device SN
 - IP Protocol: tcp
 - Log Action
 - Generated Time: 2014/03/25 11:02:57
 - Start Time: 2014/03/25 11:02:50
 - Receive Time: 2014/03/25 11:02:58
 - Elapsed Time(sec): 5
- Source:**
 - User: 11.11.11.1
 - Address: 11.11.11.1
 - Country: US
 - Port: 41220
 - Zone: l3trust
 - Interface: ethernet1/1
- Destination:**
 - User: 11.11.11.2
 - Address: 11.11.11.2
 - Country: US
 - Port: 80
 - Zone: l3trust
 - Interface: ethernet1/1
- Details:**
 - Bytes: 134
 - Bytes Received: 60
 - Bytes Sent: 74
 - Repeat Count: 1
 - Packets: 2
 - Packets Received: 1
 - Packets Sent: 1
- Flags:**
 - Captive Portal:
 - Proxy Transaction:
 - Decrypted:
 - Packet Capture:
 - Client to Server:
 - Server to Client:
 - Symmetric Return:
 - Mirrored:
- Related Logs (+/- 24 Hours):**

PCAP	Receive Time	Log	Type	Application	Action	Rule	Bytes	packets	Severity	Category	URL/...
	2014/03/25 11:02:58	TRAFFIC	end	incomplete	allow	rule1	134	2		any	

A 'Close' button is located at the bottom right of the window.

If the source or destination has an IP address to name mapping defined in the **Addresses** page, the name is presented instead of the IP address. To view the associated IP address, move your cursor over the name.

Review the following information in each log.

Table 179. Log Descriptions

Chart	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>Click  next to an entry to view additional details about the session, such as whether an ICMP entry aggregates multiple sessions between the same source and destination (the Count value will be greater than one).</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>
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>Click  next to an entry to view additional details about the threat, such as whether the entry aggregates multiple threats of the same type between the same source and destination (the Count value will be greater than one).</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>If local packet captures are enabled, click  next to an entry to access the captured packets, as in the following figure. To enable local packet captures, see the subsections under “Security Profiles”.</p>
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. You can enable logging of the HTTP header options for the URL. See “URL Filtering Profiles” for information on defining URL filtering profiles.</p>
WildFire Submissions	<p>Displays logs for files that are uploaded and analyzed by the WildFire server, log data is sent back to the device after analysis, along with the analysis results.</p>
Data Filtering	<p>Displays logs for the security policies that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall. See “Data Filtering Profiles” for information on defining data filtering profiles.</p> <p>To configure password protection for access the details for a log entry, click the  icon. Enter the password and click OK. See “Defining Custom Response Pages” for instructions on changing or deleting the data protection password.</p> <p>Note: <i>The system prompts you to enter the password only once per session.</i></p> <p>This log also shows information for file blocking profiles. For example, if you are blocking .exe files, the log will show that the files that were blocked. If you forward files to WildFire, you will see the results of that action. In this case, if you are forwarding PE files to WildFire for example, the log will show that the file was forwarded and will also show the status on whether or not it was uploaded to WildFire successfully or not.</p>

Table 179. Log Descriptions (Continued)

Chart	Description
Configuration	Displays an entry for each configuration change. Each entry includes the date and time, the administrator user name, the IP address from where the change was made, the type of client (Web or CLI), the type of command executed, whether the command succeeded or failed, the configuration path, and the values before and after the change.
System	Displays an entry for each system event. Each entry includes the date and time, the event severity, and an event description.
HIP Match	Displays information about security policies that apply to GlobalProtect clients. For more information, see “Setting Up the GlobalProtect Portal” .
Alarms	The alarms log records detailed information on alarms that are generated by the system. The information in this log is also reported in the Alarms window. See “Defining Alarm Log Settings” .

Viewing Session Information

- ▶ *Monitor > Session Browser*

Open the **Session Browser** page to browse and filter current running sessions on the firewall. For information on filtering options for this page, see [“Viewing the Logs”](#).

Working with Botnet Reports

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

- [“Managing Botnet Reports”](#)
- [“Configuring the Botnet Report”](#)

Managing Botnet Reports

- ▶ *Monitor > Botnet > Report Setting*

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

Table 180. Botnet Report Settings

Field	Description
Test Run Time Frame	Select the time interval for the report: Last 24 Hours (the default) or Last Calendar Day .
Run Now	Click the button to manually generate the report immediately. The dialog displays the report in a new tab.
No. of Rows	Specify the number of rows in the report (default is 100).
Scheduled	Select the check box to automatically generate the report daily. By default, the check box is enabled.
Query Builder	<p>For each query that you want the report to run, complete the following fields and click Add.</p> <ul style="list-style-type: none"> • Connector—Select a logical connector (and/or). Selecting the Negate check box applies negation to the query: the report will exclude the hosts that the query specifies. • Attribute—Select a zone, address, or user that is associated with the hosts that the firewall evaluates for botnet activity. • Operator—Select an operator to relate the Attribute to a Value. • Value—Enter a value for the query to match.

Configuring the Botnet Report

► *Monitor > Botnet*

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

Table 181. Botnet Configuration Settings

Field	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—Identifies users communicating with known malware URLs based on malware and botnet URL filtering categories. • Use of dynamic DNS—Looks for traffic that is destined for dynamic DNS sites, which might indicate botnet communication. • Browsing to IP domains—Identifies users who browse to IP domains instead of URLs. • Browsing to recently registered domains—Looks for traffic to domains that were registered within the past 30 days. • Executable files from unknown sites—Identifies executable files downloaded from unknown URLs.

Table 181. Botnet Configuration Settings (Continued)

Field	Description
Unknown Applications	Define the thresholds that determine whether the report will include traffic associated with suspicious Unknown TCP or Unknown UDP applications. <ul style="list-style-type: none">• Sessions Per Hour—The report includes traffic that involves up to the specified number of application sessions per hour.• Destinations Per Hour—The report includes traffic that involves up to the specified number of application destinations per hour.• Minimum Bytes—The report includes traffic for which the application payload equals or exceeds the specified size.• Maximum Bytes—The report includes traffic for which the application payload is equal to or less than the specified size.
IRC	Select the check box to include traffic involving IRC servers.

Managing PDF Summary Reports

► *Monitor > PDF Reports > Manage PDF Summary*

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

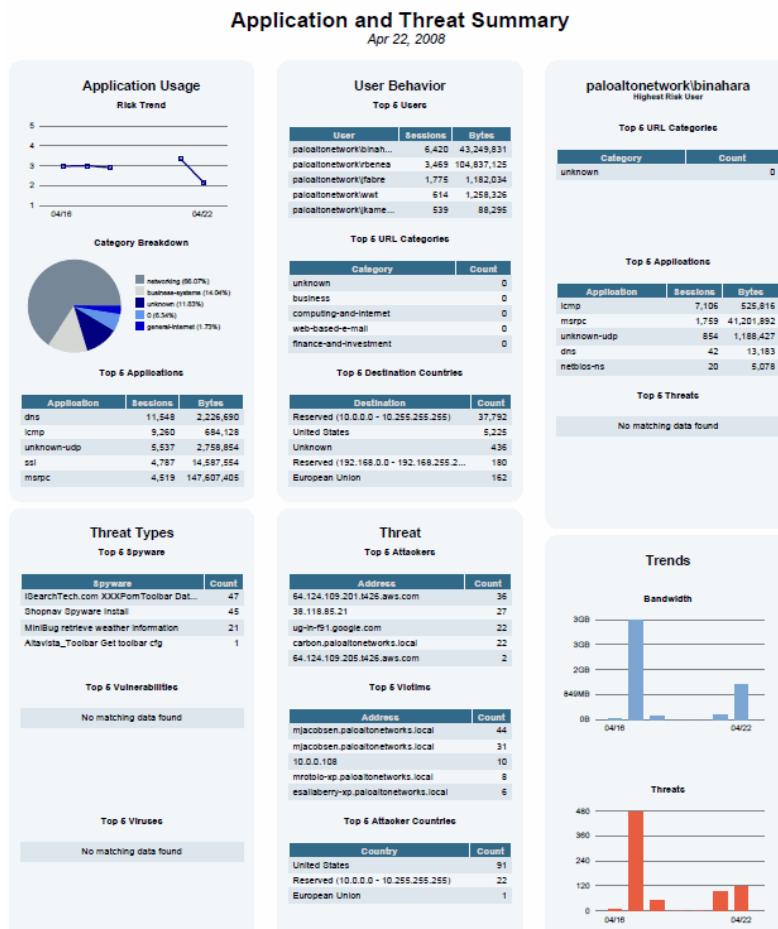


Figure 13. PDF Summary Report

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

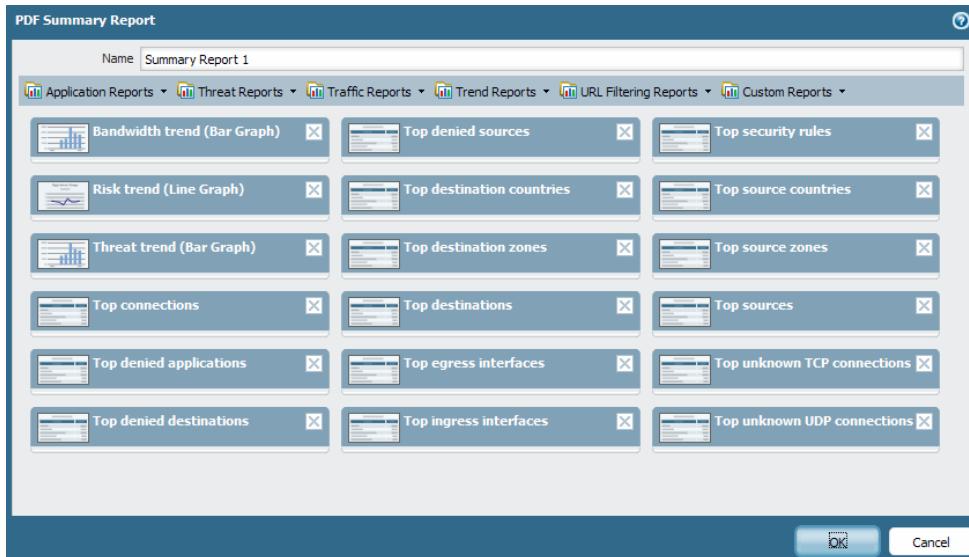


Figure 14. Managing PDF Reports

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

- To remove an element from the report, click the icon in the upper-right corner of the element's icon box or remove the check box from the item in the appropriate drop-down list box near the top of the page.
- Select additional elements by choosing from the drop-down list boxes near the top of the page.
- Drag and drop an element's icon box to move it to another area of the report.



A maximum of 18 report elements is permitted. You may need to delete existing elements to add additional ones.

Click **Save**, enter a name for the report, as prompted, and click **OK**.

To display PDF reports, choose **PDF Summary Report**, and select a report type from the drop-down list at the bottom of the page to display the generated reports of that type. Click an underlined report link to open or save the report.

Managing User/Group Activity Reports

► *Monitor > PDF Reports > User Activity Report*

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

Table 182. User/Group Activity Report Settings

Field	Description
Name	Enter a name to identify the report (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Type	<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.</p> <p>On Panorama, you must have set up a master device for each device group in order to retrieve user group information for generating the report.</p>
	<p>For Group Activity Report: Select Group and enter the Group Name.</p> <p>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 list.
Include Detailed Browsing	<p>Select this option only if you wish to include detailed URL logs in the report.</p> <p><i>The detailed browsing information can include a large volume of logs (thousands of logs) for the selected user or user group and can make the report very large.</i></p>

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

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

To save the report, click **OK**. You can then schedule the report for email delivery, see “[Scheduling Reports for Email Delivery](#)”.

Managing Report Groups

► *Monitor > PDF Reports > Report Groups*

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

Table 183. Report Group Settings

Field	Description
Name	Enter a name to identify the report group (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Title Page	Select the check box to include a title page in the report.
Title	Enter the name that will appear as the report title.
Report selection	Select reports from the left column and click Add to move each report to the report group on the right. You can select Predefined, Custom, PDF Summary, and Log View report types. The Log View report is a report type that is automatically created each time you create a custom report and uses the same name as the custom report. This report will show the logs that were used to build the contents of the custom report. To include the log view data, when creating a report group, you add your custom report under the Custom Reports list and then add the log view report by selecting the matching report name from the Log View list. When you receive the report, you will see your custom report data followed by the log data that was used to create the custom report.

To use the report group, see “[Scheduling Reports for Email Delivery](#)”.

Scheduling Reports for Email Delivery

► *Monitor > PDF Reports > Email Scheduler*

Use the Email scheduler to schedule reports for delivery by email. Before adding a schedule, you must define report groups and an email profile. See “[Managing Report Groups](#)” and “[Configuring Email Notification Settings](#)”.

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

Table 184. Email Scheduler Settings

Field	Description
Name	Enter a name to identify the schedule (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Report Group	Select the report group (see “ Managing Report Groups ”).
Recurrence	Select the frequency at which to generate and send the report.
Email Profile	Select the profile that defines the email settings. See “ Configuring Email Notification Settings ” for information on defining email profiles.
Override Recipient email(s)	Enter an optional email address to use instead of the recipient specified in the email profile.

Viewing Reports

► *Monitor > Reports*

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

To view the reports, click the report names on the right side of the page (Custom Reports, Application Reports, Traffic Reports, Threat Reports, URL Filtering Reports, and PDF Summary Reports).

By default, all reports are displayed for the previous calendar day. To view reports for any of the previous days, select a report generation date from the **Select** drop-down list at the bottom of the page.

The reports are listed in sections. You can view the information in each report for the selected time period. To export the log in CSV format, click **Export to CSV**. To open the log information in PDF format, click **Export to PDF**. The PDF file opens in a new window. Click the icons at the top of the window to print or save the file.

Generating Custom Reports

► *Monitor > Manage Custom Reports*

You can create custom reports that are optionally based on existing report templates. The reports can be run on demand or scheduled to run each night. To view previously defined reports, choose **Reports** on the side menu.

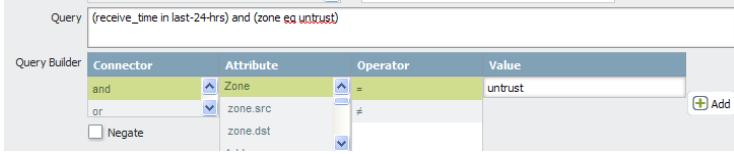
Click **Add** to create a new custom report. To base a report on an existing template, click **Load Template** and choose the template.

Specify the following settings to define the report.

Table 185. Custom Report Settings

Field	Description
Name	Enter a name to identify the report (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Database	Choose the database to use as the data source for the report.
Time Frame	Choose a fixed time frame or choose Custom and specify a date and time range.
Sort By	Choose sorting options to organize the report, including the amount of information to include in the report. The available options depend on the choice of database.
Group By	Choose grouping options to organize the report, including the amount of information to include in the report. The available options depend on the choice of database.
Scheduled	Select the check box to run the report each night. The report then becomes available by choosing Reports on the side menu.
Columns	Choose the columns to include in the custom report from the Available Column list and use the plus icon to move them to the Selected Columns list. Use the up and down arrows to reorder the selected columns, and use the minus icon to remove previously selected columns.

Table 185. Custom Report Settings (Continued)

Field	Description
Query Builder	<p>To build a report query, specify the following and click Add. Repeat as needed to construct the full query.</p> <ul style="list-style-type: none"> • Connector—Choose the connector (and/or) to precede the expression you are adding. • Negate—Select the check box to interpret the query as a negation. In the previous example, the negate option causes a match on entries that are not in the past 24 hours or are not from the “untrust” zone. • Attribute—Choose a data element. The available options depend on the choice of database. • Operator—Choose the criterion to determine whether the attribute applies (such as =). The available options depend on the choice of database. • Value—Specify the attribute value to match. <p>For example, the following figure (based on the Traffic Log database) shows a query that matches if the traffic log entry was received in the past 24 hours and is from the “untrust” zone.</p> 

Taking Packet Captures

► Monitor > Packet Capture

PAN-OS supports packet capture for troubleshooting or detecting unknown applications. You can define filters such that only the packets that match the filters are captured. The packet captures are locally stored on the device and are available for download to your local computer.



Packet Capture is for troubleshooting only. This feature can cause the system performance to degrade and should be used only when necessary. After the capture is complete, please remember to disable the feature.

To specify filtering and capture options, specify the information in the following table.

To clear all filtering and capture settings, click **Clear All Settings**.

To select capture files for download, click the file name in the capture file list on the right side of the page.

Table 186. Packet Capture Settings

Field	Description
Configure Filtering	
Manage Filters	<p>Click Manage Filters, click Add to add a new filter, and specify the following information:</p> <ul style="list-style-type: none"> • Id—Enter or select an identifier for the filter. • Ingress Interface—Select the firewall interface. • Source—Specify the source IP address. • Destination—Specify the destination IP address. • Src Port—Specify the source port. • Dest Port—Specify the destination port. • Proto—Specify the protocol to filter. • 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). • IPv6—Select the check box to include IPv6 packets in the filter.
Filtering	Click to toggle the filtering selections on or off.
Pre-Parse Match	<p>Click to toggle the pre-parse match option on or off.</p> <p>The pre-parse-match option is added 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.</p> <p>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.</p> <p>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 even the 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.</p>

Table 186. Packet Capture Settings (Continued)

Field	Description
Configuring Capturing	
Packet Capture	Click to toggle packet capturing on or off.
Packet Capture Stage	Click Add and specify the following: <ul style="list-style-type: none"> • Stage—Indicate the point at which to capture the packet: <ul style="list-style-type: none"> – drop—When packet processing encounters an error and the packet is to be 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 to be 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. • Packet Count—Specify the number of packets after which capturing stops. • Byte Count—Specify the number of bytes after which capturing stops.
Captured Files	
Captured Files	Click Delete to remove a packet capture file from the list displaying captured files.
Settings	
Clear All Settings	Click Clear All Settings to clear all packet capture settings.

Chapter 7

Configuring the Firewall for User Identification

- “Configuring the Firewall for User Identification”
- “User Mapping Tab”
- “User-ID Agents Tab”
- “Terminal Services Agents Tab”
- “Group Mapping Tab”
- “Captive Portal Settings Tab”

Configuring the Firewall for User Identification

► *Device > User Identification*

User Identification (User-ID) is a Palo Alto Networks next-generation firewall feature that allows you to create policies and perform reporting based on users and groups rather than individual IP addresses. If you are configuring a firewall with multiple virtual systems, you must create a separate User-ID configuration for each virtual system; user mapping information is not shared between virtual systems. Select the virtual system you want to configure for User-ID from the **Location** drop-down at the top of the User Identification page. After selecting a virtual system (if applicable), use the settings on this page to configure the user identification settings.

- “User Mapping Tab”
- “User-ID Agents Tab”
- “Terminal Services Agents Tab”
- “Group Mapping Tab”
- “Captive Portal Settings Tab”

User Mapping Tab

Use the **User Mapping** tab to configure a firewall to retrieve IP address-to-username mapping data directly from domain servers. This feature does not require the installation of a User-ID Agent on the domain servers. The firewall can also be configured to redistribute the user mapping information to other firewalls.

Table 187. User Mapping Settings

Field	Description
Palo Alto Networks User ID Agent Setup	
	<p>This section of the screen shows the settings the firewall will use to perform IP address to user mapping. To configure or edit the settings, click the Edit  icon to open the setup dialog, which contains the following subtabs:</p> <ul style="list-style-type: none"> • WMI Authentication • Server Monitor • Client Probing • Cache • NTLM • Redistribution • Syslog Filters
WMI Authentication subtab	<p>Use this subtab to set the domain credentials for the account the firewall will use to access Windows resources. This is required for monitoring Exchange servers and domain controllers as well as for WMI probing.</p> <p>User Name—Specify the account that has permissions to perform WMI queries on client computers and server monitoring. Enter the user name using the domain\username syntax.</p> <p>Password/Confirm Password—Specify the account password.</p>

Table 187. User Mapping Settings (Continued)

Field	Description
Server Monitor subtab	<p>Enable Security Log—Select the check box to enable security log monitoring on Windows servers. Security logs will be queried to locate IP address to username mapping information on the servers specified in the Server Monitoring list.</p> <p>Server Log Monitor Frequency (sec)—Specify the frequency in seconds at which the firewall will query Windows server security logs for IP address to username mapping information (default is 2, range is 1-3600). This is the interval between when the firewall finishes processing the last query and when it starts the next query.</p> <p>Enable Session—Select the check box to enable monitoring of user sessions on the servers specified in the Server Monitoring list. Each time a user connects to a server, a session is created and this information can also be used to identify the user IP address.</p> <p>Server Session Read Frequency (sec)—Specify the frequency in seconds at which the firewall will query Windows server user sessions for IP address to username mapping information (default is 10, range is 1-3600). This is the interval between when the firewall finishes processing the last query and when it starts the next query.</p> <p>Novell eDirectory Query Interval (sec)—Specify the frequency in seconds at which the firewall will query Novell eDirectory servers for IP address to username mapping information (default is 30, range is 1-3600). This is the interval between when the firewall finishes processing the last query and when it starts the next query.</p> <p><i>Note:</i> 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.</p>
Client Probing subtab	<p>Enable Probing—Select this check box to enable WMI/NetBIOS probing to each client PC identified by the user mapping process. Probing will help ensure that the same user is still logged into the client PC in order to provide accurate user to IP information.</p> <p>Probe Interval (min)—Specify the client PC probe interval (default is 20, range is 1-1440). This is the interval between when the firewall finishes processing the last request and when it starts the next request.</p> <p>In large deployments, it is important to set the probe interval properly to allow time to probe each client that has been identified. Example, if you have 6,000 users and an interval of 10 minutes, it would require 10 WMI request a second from each client.</p> <p><i>Note:</i> If the probe request load is high, the observed delay between requests might significantly exceed the interval you specify.</p> <p><i>Note:</i> For WMI polling to work effectively, the User Mapping profile must be configured with a domain administrator account, and each probed client PC must have a remote administration exception configured in the Windows firewall. For NetBIOS probing to work effectively, each probed client PC must allow port 139 in the Windows firewall and must also have file and printer sharing services enabled.</p>

Table 187. User Mapping Settings (Continued)

Field	Description
Cache subtab	<p>Enable User Identification Timeout—Select this check box to enable a timeout value for IP address-to-username mapping entries. When the timeout value is reached, the IP address-to-username mapping will be cleared and a new mapping will be collected. This will ensure that the firewall has the most current information as users roam around and obtain new IP addresses.</p> <p>User Identification Timeout (min)—Set the timeout value for IP address-to-username mapping entries (default 45 minutes; range 1-1440 minutes).</p>
NTLM subtab	<p>Enable NTLM authentication processing—Select this check box to enable NT LAN Manager (NTLM) authentication processing. When Captive Portal rules have an action set to browser-challenge (see “Defining Captive Portal Policies”) to capture user mapping information, an NTLM challenge transparently authenticates the client. With this option enabled, the firewall collects this information from the NTLM domain.</p> <p>When you configure the firewall to share its User-ID information with other PAN-OS firewalls (see “Redistribution subtab”), it can serve NTLM requests coming from those firewalls, performing the function of the User-ID agent.</p> <p><i>Note:</i> If you use the Windows-based User-ID agent, NTLM responses go directly to the domain controller where you installed the agent.</p> <p>NTLM Domain—Enter the NTLM domain name.</p> <p>Admin User Name—Enter the administrator account that has access to the NTLM domain.</p> <p>WARNING: Do not include the domain in the Admin User Name field. Otherwise, the firewall will fail to join the domain.</p> <p>Password/Confirm Password—Enter the password for the administrator account that has access to NTLM domain.</p> <p><i>Note:</i> You can only enable NTLM authentication processing on one virtual system (you select the virtual system from the Location drop-down at the top of the page).</p>
Redistribution subtab	<p>Collector Name—Specify the collector name if you want this firewall to act as a user mapping redistribution point for other firewalls on your network.</p> <p>The collector name and pre-shared key are used when configuring the User-ID Agents on the firewalls that will pull the user mapping information.</p> <p>To enable a firewall to act as a re-distribution point, you also need to enable User-ID service in Network > Network Profiles > Interface Mgmt.</p> <p>Pre-Shared Key/Confirm Pre-Shared Key—Enter the pre-shared key that is used by other firewalls to establish a secure connection for user mapping transfers.</p>

Table 187. User Mapping Settings (Continued)

Field	Description
Syslog Filters subtab	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>Tip: 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.</p> <p>Note: The complete procedure to configure the User-ID agent to collect user mapping information from a syslog sender requires additional tasks. To configure a custom Syslog Parse profile, click Add and complete the following fields.</p> <ul style="list-style-type: none"> • Syslog Parse Profile—Enter a name for the profile (up to 63 alphanumeric characters). • Description—Enter a description for the profile (up to 255 alphanumeric characters). • Type—Specify the type of parsing to identify successful authentication events: "Regex Identifier" and "Field Identifier". <p>The remaining fields in the dialog vary based on your Type selection. Configure the fields for the desired type as described in the following rows. The field descriptions in this table use a login event example from a syslog message with the following format:</p> <pre>[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success User:domain\johndoe_4 Source:192.168.0.212</pre>

Table 187. User Mapping Settings (Continued)

Field	Description
Syslog Filters tab (Continued)	<p>Regex Identifier 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.</p> <ul style="list-style-type: none"> • Event Regex—Enter the regex to match successful authentication events. For the sample message, the regex (authentication\s+success){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:(\w+\.\w+)</code> matches the string <code>User:johndoe_4</code> and extracts <code>johndoe_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:(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{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.
Syslog Filters tab (Continued)	<p>Field Identifier Specify strings to match the authentication event and identify the user mapping information in syslog messages.</p> <ul style="list-style-type: none"> • 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 <code>\s</code> (for a space) or <code>\t</code> (for a tab). In the sample message, <code>User:</code> identifies the start of the username field. • Username Delimiter—Enter the delimiter that indicates the end of the username field in syslog messages. Use <code>\s</code> to indicate a standalone space (as in the sample message) and <code>\t</code> 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 <code>\s</code> (for a space) or <code>\t</code> (for a tab). In the sample message, <code>Source:</code> 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 <code>\n</code> to indicate the delimiter is a line break.

Table 187. User Mapping Settings (Continued)

Field	Description
Server Monitoring	<p>Note: Keep in mind that in order for AD events to be recorded in the security log, the AD domain must be configured to log successful account logon events.</p> <p>Use this section of the screen to define the Microsoft Exchange Servers, domain controllers, Novell eDirectory servers or syslog senders to monitor for logon events. For example, in an AD environment, the agent will monitor the security logs for Kerberos ticket grants or renewals, Exchange server access (if configured), and file and print service connections (for monitored servers). You can define entries for a total of up to 100 monitored servers, including syslog senders, Microsoft Active Directory, Microsoft Exchange, or Novell eDirectory servers.</p>

Table 187. User Mapping Settings (Continued)

Field	Description
Include/Exclude Networks	
	By default, if you do not specify subnetworks in this list, User-ID will perform IP address to username mapping (discovery) for all the subnetworks of the servers in the Server Monitoring list. To limit discovery to specific subnetworks, click Add and specify a profile that comprises a Name , subnetwork IP address range (Network Address), Discovery option (Include or Exclude) , and Enabled option (by which to enable or disable the profile). User-ID applies an implicit exclude all rule to the list. For example, if you add subnetwork 10.0.0.0/8 with the Include option, User-ID excludes all other subnetworks even if you do not add them to the list. Add entries with the Exclude option only if you want User-ID to exclude a subset of the subnetworks you explicitly included. For example, if you add 10.0.0.0/8 with the Include option and add 10.2.50.0/22 with the Exclude option, User-ID will perform discovery on all the subnetworks of 10.0.0.0/8 except 10.2.50.0/22, and will exclude all subnetworks outside of 10.0.0.0/8. Note that if you add Exclude profiles without adding any Include profiles, User-ID excludes all subnetworks, not just the ones you added.
	By default, User-ID evaluates the profiles in the order you add them, from top-first to bottom-last. To change the evaluation order, click Custom Include/Exclude Network Sequence . In the dialog that opens, Add , Delete , Move Up , or Move Down the profiles to create a custom evaluation order.
	If you configure the firewall to distribute user mapping information to other firewalls, the discovery limits you specify in the Include/Exclude Networks list will apply to the distributed information.
	To apply the user mapping information to firewall traffic so that the information is available in logs, reports, and policies, you must Enable User Identification in each security zone (see “ Defining Security Zones ”).

User-ID Agents Tab

Use the **User-ID Agents** tab to configure the firewall to interact with User Identification Agents (User-ID Agents) installed on directory servers on your network or with firewalls configured for agentless User-ID for the exchange of IP address to user mapping information.

A User-ID Agent collects IP address-to-username mapping information from network resources and provides it to the firewall for use in security policies and logs.



User identification mapping requires that the firewall obtain the source IP address of the user before the IP address is translated with NAT. If multiple users appear to have the same source address, due to NAT or use of a proxy device, accurate user identification is not possible.

In environments where other network devices are already authenticating users, you can configure the authenticating service to forward event logs to the User-ID agent using syslog. The agent can then extract the authentication events from the syslogs and add them to the User-ID IP address-to-username mappings.

To add a new User-ID agent to the list of agents this firewall communicates with, click **Add** and complete the following fields.

Table 188. User-ID Agents Settings

Field	Description
Name	Enter a name to identify the User-ID Agent (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Host	Enter the IP address of the Windows host on which the User-ID Agent is installed.
Port	Enter the port number on which the User-ID Agent service is configured to listen for requests from the firewall. The default Windows User-ID agent service port number is 5007, however you can use any available port as long as the firewall and the User-ID Agent service are using the same value. In addition, you can use different port numbers on different agents. <i>Note: Some earlier versions of the User-ID agent use 2010 as the default port.</i>
Collector Name	If this firewall is receiving user mapping information from another firewall that is configured for redistribution, specify the collector name configured on the firewall that will be collecting the user mapping data (this is displayed on the Device > User Identification > User Mapping tab).
Collector Pre-shared Key/Confirm Collector Pre-shared key	Enter the pre-shared key that will be used to allow SSL connectivity between the User-ID Agent and the firewall that is acting as a distribution point for user mapping.
Use as LDAP Proxy	Select the check box to use this User-ID agent as a proxy for collecting group mapping information from a directory server and forwarding it to the firewall. To use this option, you must also configure group mapping on the firewall (see “ Group Mapping Tab ”). The firewall will push that configuration to the User-ID agent to enable it to collect the mapping information. This option is useful in deployments where the firewall cannot directly access the directory server. It is also useful in deployments that benefit from reducing the number of queries the directory server must process; multiple firewalls can receive the group mapping information from the cache on a single User-ID agent instead of each firewall directly querying the server.

Table 188. User-ID Agents Settings (Continued)

Field	Description
Use for NTLM Authentication	Select the check box to use the configured User-ID Agent to verify NTLM client authentication from the captive portal with the Active Directory domain.
Enabled	<p>Select the check box to enable the firewall to communicate with this user identification agent.</p> <p>To finish adding the User-ID agent entry, click OK. The new User-ID agent is displayed on the list of agents. Verify that the icon in the Connected column is green, indicating that the firewall can successfully communicate with the agent. A yellow icon indicates a disabled connection and a red icon indicates a failed connection.</p> <p>If you think the connection status might have changed since you first opened the page, click Refresh Connected to update the status display.</p> <p>If you want the firewall to communicate with agents in a specific order—for example, based on the proximity of the agents to the firewall or whether an agent is a backup or primary—click Custom Agent Sequence and then order the agents in the preferred order.</p>

Terminal Services Agents Tab

Use the **Terminal Services Agents** tab to configure the firewall to interact with Terminal Services Agents (TS Agents) installed on your network. The TS Agent identifies individual users who are supported by the same terminal server and thus appear to have the same IP address. The TS Agent on a terminal server identifies individual users by allocating a specific port range to each individual user. When a port range is allocated for a particular user, the Terminal Services Agent notifies every connected firewall about the allocated port range so that policy can be enforced based on user and user groups.

To add a TS Agent to the firewall configuration, click **Add** and then complete the following fields:

Table 189. Terminal Services Agents Settings

Field	Description
Name	Enter a name to identify the TS Agent (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Host	Enter the IP address of the terminal server on which the TS Agent is installed.
Port	Enter the port number on which the TS Agent service is configured to communicate with the firewall. The default port is 5009.

Table 189. Terminal Services Agents Settings (Continued)

Field	Description
Alternative IP Addresses	If the terminal server where the TS Agent is installed has multiple IP addresses that can appear as the source IP address for the outgoing traffic, click Add and then enter up to eight additional IP addresses.
Enabled	Select the check box to enable the firewall to communicate with this user identification agent. To finish adding the TS Agent entry, click OK . The new TS Agent is displayed on the list of agents. Verify that the icon in the Connected column is green, indicating that the firewall can successfully communicate with the agent. A yellow icon indicates a disabled connection and a red icon indicates a failed connection. If you think the connection status might have changed since you first opened the page, click Refresh Connected to update the status display.

Group Mapping Tab

In order to define security policies based on user or group, the firewall must retrieve the list of groups and the corresponding list of members from your directory server. To enable this functionality, you must create an LDAP server profile that instructs the firewall how to connect and authenticate to the LDAP directory server. The firewall supports a variety of LDAP directory servers, including Microsoft Active Directory (AD), Novell eDirectory, and Sun ONE Directory Server.

After creating the server profile, use the **Group Mapping** tab to define how to search the directory for the user and group information.

To add a group mapping configuration click **Add** and then enter a unique **Name** to identify the configuration. The name is case-sensitive and can be up to 31 characters, including letters, numbers, spaces, hyphens, and underscores. You must then complete the fields on the following subtabs:

- “[Server Profile Subtab](#)”
- “[Group Include List Subtab](#)”

Server Profile Subtab

Use the Server Profile subtab to select an LDAP server profile to use for group mapping and specify how to search the directory for the specific objects that contain the user and group information

Table 190. Group Mapping Server Profile Settings

Field	Description
Server Profile	Select the LDAP server profile to use for group mapping on this firewall. For instructions on creating an LDAP Server Profile, see the PAN-OS Administrator's Guide .
Update Interval	Specify the interval (seconds) after which the firewall will initiate a connection with the LDAP directory server to obtain any updates that have been made to the groups that are used in firewall policy (Range 60 to 86,400 seconds).

Table 190. Group Mapping Server Profile Settings (Continued)

Field	Description
Group Objects	<ul style="list-style-type: none"> Search Filter—Specify an LDAP query that can be used to control which groups are retrieved and tracked. Object Class—Specify the definition of a group. For example, the default is objectClass=group, which means that the system retrieves all objects in the directory that match the group filter and have objectClass=group. Group Name—Enter the attribute that specifies the name of the group. For example in Active Directory, this attribute is “CN” (Common Name). Group Member—Specify the attribute that contains the members of this group. For example in Active Directory, this attribute is “member.”
User Objects	<ul style="list-style-type: none"> Search Filter—Specify an LDAP query that can be used to control which users are retrieved and tracked. Object Class—Specify the definition of the a user object. For example in Active Directory, the objectClass is “user.” User Name—Specify the attribute for user name. For example, in Active Directory, the default user name attribute is “samAccountName.”
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 information collected by User-ID. The log will contain a link to the user and when clicked, the ACC is displayed and filtered by the user. If the email is sent to a distribution list, the ACC is filtered by the members contained in the list.</p> <p>The email header and User-ID information will help you quickly track down and thwart threats that arrive via email by making it easier to identify the user(s) who received the email.</p> <ul style="list-style-type: none"> Mail Attributes—This field is automatically populated based on the LDAP server type (Sun/RFC, Active Directory, and Novell). Domain List—Enter the list of email domains in your organization using a comma separated list up to 256 characters.
Enabled	To enable this server profile for group mapping, make sure this check box is selected.

Group Include List Subtab

Use the **Group Include List** subtab to limit the number of groups are displayed when creating a security policy. Browse through the LDAP tree to locate the groups you want to be able to use in policy. For each group you want to include, select it in the **Available Groups** list and click the add  icon to move it to the **Included Groups** list. Click the  icon to remove groups from the list. Repeat this step for every group you want to be able to use in your policies and then click **OK** to save the list of included groups.

Captive Portal Settings Tab

Use the **Captive Portal Settings** tab to configure captive portal authentication on the firewall. If the firewall receives a request from a zone that has User-ID enabled and the source IP address does not have any user data associated with it yet, it checks its Captive Portal policy for a match to determine whether to perform authentication. This is useful in environments where you have clients that are not logged in to your domain servers, such as Linux clients. This user mapping method is only triggered for web traffic (HTTP or HTTPS) that matches a

security rule/policy, but that has not been mapped using a different method. For non-web-based traffic or traffic that does not match a captive portal policy, the firewall uses its IP-based security policies rather than the user-based policies.

To configure or edit the captive portal configuration, click the Edit  icon and then complete the following fields:

Table 191. Captive Portal Settings

Field	Description
Enabled	Select this check box to enable the captive portal option for user identification.
Idle Timer (min)	This is the user time to live (user TTL) setting for a captive portal session. This timer resets every time there is activity from a captive portal user. If the length of time the user is idle exceeds the idle timer, the captive portal user mapping will be removed and the user will have to log in again. (1-1440 minutes, default 15 minutes).
Expiration (min)	This is the maximum TTL, which is the maximum amount of time that any captive portal session can remain mapped. After the expiration duration has elapsed, the mapping will be removed and users will have to re-authenticate even if the session is active. This timer is used to ensure prevent stale mappings and the value set here overrides the idle timeout. Therefore, as a best practice, set the expiration to a value that is higher than the idle timer (range 1 - 1440 minutes; default 60 minutes).
Redirect Host	(Redirect mode only) Specify the intranet hostname that resolves to the IP address of the Layer 3 interface to which you are redirecting requests.
Server Certificate	(Redirect mode only) Select the server certificate the firewall should use to redirect requests over SSL. To transparently redirect users without displaying certificate errors, install a certificate that matches the IP address of the interface to which you are redirecting requests. You can either generate a self-signed certificate or import a certificate that is signed by an external CA. <i>Note: If you select None, the firewall will use the local default certificate for SSL connections.</i>
Authentication Profile	Select the authentication profile to use to authenticate users who are redirected to a web form for authentication. Note that even if you plan to use NTLM for authentication, you must configure either an authentication profile or a certificate profile to authenticate users if NTLM authentication fails or cannot be used because the client or browser does not support it.

Table 191. Captive Portal Settings (Continued)

Field	Description
Mode	<p>Select one of the following modes to define how web requests are captured for authentication:</p> <ul style="list-style-type: none"> • Transparent—The firewall intercepts the browser traffic per the Captive Portal rule and impersonates the original destination URL, issuing an HTTP 401 to invoke authentication. However, because the firewall does not have the real certificate for the destination URL, the browser will display a certificate error to users attempting to access a secure site. Therefore you should only use this mode when absolutely necessary, such as in Layer 2 or virtual wire deployments. • Redirect—The firewall intercepts unknown HTTP or HTTPS sessions and redirects them to a Layer 3 interface on the firewall using an HTTP 302 redirect in order to perform authentication. This is the preferred mode because it provides a better end-user experience (no certificate errors). However, it does require additional Layer 3 configuration. Another benefit of the Redirect mode is that it provides for the use of session cookies, which enable the user to continue browsing to authenticated sites without requiring re-mapping each time the time outs expire. This is especially useful for users who roam from one IP address to another (for example, from the corporate LAN to the wireless network) because they will not need to re-authenticate upon IP address change as long as the session stays open. In addition, if you plan to use NTLM authentication, you must use Redirect mode because the browser will only provide credentials to trusted sites. <p><i>To use the captive portal in redirect mode, you must enable response pages on the interface management profile assigned to the Layer 3 interface to which you are redirecting the active portal. See “Defining Interface Management Profiles” and “Configuring a Layer 3 Ethernet Interface”.</i></p>
Session Cookie	<ul style="list-style-type: none"> • Enable—Select the check box to enable session cookies. This option is only valid if you selected Redirect as the Mode. • Timeout—If session cookies are enabled, this timer specifies the number of minutes the session cookie is valid. (range 60 - 10080 minutes; default 1440 minutes). • Roaming—Select the check box if to retain the cookie if the IP address changes while the session is active (for example, if the client moves from a wired to wireless network). The user will only have to re-authenticate if the cookie times out or the user closes the browser.

Table 191. Captive Portal Settings (Continued)

Field	Description
Certificate Profile	Select a Certificate Profile for authenticating Captive Portal users (see "Creating a 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.
NTLM Authentication	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>Note: 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 NTLM authentication in the PAN-OS integrated User-ID agent setup (NTLM subtab) and provide the credentials for the firewall to join the domain. NTLM is available only for Windows Server version 2003 and earlier versions.</p> <p>To configure NTLM for use with Windows-based User-ID agents, define the following:</p> <ul style="list-style-type: none"> • Attempts—Specify the number of attempts after which the NTLM authentication fails (Range 1-60; default 1). • Timeout—Specify the number of seconds after which the NTLM authentication times out (Range 1-60 seconds; default 2 seconds). • Reversion Time—Specify the time after which the firewall will again try to contact the first agent in the list of User-ID Agents after the agent becomes unavailable (Range 60-3600 seconds; default 300 seconds).

Chapter 8

Configuring IPSec Tunnels

This section describes basic virtual private network (VPN) technology and provides details on configuring IP Security (IPSec) VPNs on Palo Alto Networks firewalls.

See the following topics:

- [“Defining IKE Gateways”](#)
- [“Setting Up IPSec Tunnels”](#)
- [“Defining IKE Crypto Profiles”](#)
- [“Defining IPSec Crypto Profiles”](#)

Defining IKE Gateways

► *Network > Network Profiles > IKE Gateways*

Use this page to define gateways that include the configuration information necessary to perform IKE protocol negotiation with peer gateways.

To configure an IKE gateway, use the following two tabs:

- [“IKE Gateway General Tab”](#)
- [“IKE Gateway Advanced Phase 1 Options Tab”](#)

IKE Gateway General Tab

Table 192. IKE Gateway General Settings

Field	Description
Name	Enter a name to identify the gateway (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Interface	Specify the outgoing firewall interface.
Local IP Address	Select the IP address for the local interface that is the endpoint of the tunnel.
Peer Type	Static IP address or dynamic option for the peer on the far end of the tunnel.
Peer IP Address	If the Static option is selected for peer type, specify the IP address for the peer on the far end of the tunnel.
Pre-Shared Key Confirm Pre-Shared Key	Enter a security key to use for authentication across the tunnel. Applies for static and dynamic peer types. Use a maximum of 255 ASCII or non-ASCII characters. Generate a key that is difficult to crack with dictionary attacks; use a pre-shared key generator, if necessary.
Local Identification	Choose from the following types and enter the value: IP address, FQDN (hostname), User FQDN (email address), KEYID (binary format ID string in HEX). If no value is specified, the local IP address will be used as the local identification value.
Peer Identification	Choose from the following types and enter the value: IP address, FQDN (hostname), User FQDN (email address), KEYID (binary format ID string in HEX). If no value is specified, the peer IP address will be used as the peer identification value.

IKE Gateway Advanced Phase 1 Options Tab

Table 193. IKE Gateway General Settings

Field	Description
Exchange Mode	Choose auto, aggressive, or main.
IKE Crypto Profile	Select an existing profile or keep the default profile.
Enable Passive Mode	Select to have the firewall respond only to IKE connections and never initiate them.
Enable NAT Traversal	Select to have UDP encapsulation used on IKE and UDP protocols, enabling them to pass through intermediate NAT devices. NAT traversal is used when NAT addressing is in place between the IPSec VPN terminating points.
Dead Peer Detection	Select the check box 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 through ICMP ping and can help restore resources that are lost when a peer is unavailable.



*When a device is set to use the **auto** exchange mode, it 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 matching exchange mode to allow it to accept negotiation requests initiated from the first device.

Setting Up IPSec Tunnels

► *Network > IPSec Tunnels*

Use the **IPSec Tunnels** page to set up the parameters to establish IPSec VPN tunnels between firewalls.

To configure an IPSec tunnel, use the following two tabs:

- “[IPSec Tunnel General Tab](#)”
- “[IPSec Tunnel Proxy ID Tab](#)”

See the following when viewing IPSec tunnel status:

- “[Viewing IPSec Tunnel Status on the Firewall](#)”

IPSec Tunnel General Tab

Table 194. IPSec General Tab Tunnel Settings

Field	Description
Name	Enter a name to identify the tunnel (up to 63 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores. The 63 character limit for this field includes the tunnel name in addition to the Proxy ID, which is separated by a colon character.
Tunnel Interface	Select an existing tunnel interface, or click New Tunnel Interface to create a new tunnel interface. For information on creating a tunnel interface, see “ Configuring a Tunnel Interface ”.
Type	Select whether to use an automatically generated or manually entered security key. Auto key is recommended.

Table 194. IPSec General Tab Tunnel Settings (Continued)

Field	Description
Auto Key	<p>If you choose Auto Key, specify the following:</p> <ul style="list-style-type: none"> • IKE Gateway—See “Defining IKE Gateways” for descriptions of the IKE gateway settings. • IPSec Crypto Profile—Select an existing profile or keep the default profile. To define a new profile, click New and follow the instructions in “Defining IPSec Crypto Profiles”. <p>Advanced</p> <ul style="list-style-type: none"> • Enable Replay Protection—Select this option to protect against replay attacks. • Copy TOS Header—Copy the (Type of Service) TOS header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original TOS information. • 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 continue to use the tunnel interface in routing decisions as if the tunnel remained active. If the fail-over action is used, the firewall will disable the tunnel interface, thereby disabling any routes in the routing table that use the interface. For more information, see “Defining Monitor Profiles”.
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—Choose an encryption option for tunnel traffic (3des, aes128, aes192, aes256, aes128ccm16, or null [no encryption]). • Key/Confirm Key—Enter and confirm an encryption key.

Table 194. IPSec General Tab Tunnel Settings (Continued)

Field	Description
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. <p>Advanced Options</p> <ul style="list-style-type: none"> • Publish all static and connected routes to Gateway—Select this option to publish all routes from the satellite device to the GlobalProtect Gateway in which this satellite is connected. • Subnet—Click Add to manually add local subnets for the satellite location. If other satellites are using the same subnet information, you must NAT all traffic to the tunnel interface IP. Also, the satellite must not share routes in this case, so all routing will be done through the tunnel IP. • External Certificate Authority—Select this option if you will use an external CA to manage certificates. Once you have your certificates generated, you will need to import them into the device and select the Local Certificate and the Certificate Profile to be used.

IPSec Tunnel Proxy ID Tab

Table 195. IPSec Tunnel General Tab Settings

Field	Description
Proxy ID	Click Add and enter a name to identify the proxy.
Local	Enter an IP address or subnet in the format <i>ip_address/mask</i> (for example, 10.1.2.1/24).
Remote	If required by the peer, enter an IP address or subnet in the format <i>ip_address/mask</i> (for example, 10.1.1.1/24).
Protocol	<p>Specify the protocol and port numbers for the local and remote ports:</p> <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. <p><i>Each configured proxy ID will count towards the IPSec VPN tunnel capacity of the firewall.</i></p>

Viewing IPSec Tunnel Status on the Firewall

► *Network > IPSec Tunnels*

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

- **Tunnel Status (first status column)**—Green indicates an IPSec SA tunnel. Red indicates that IPSec SA is not available or has expired.
- **IKE Gateway Status**—Green indicates a valid IKE phase-1 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). Red indicates that the tunnel interface is down, because the tunnel monitor is enabled and the status is down.

Defining IKE Crypto Profiles

► *Network > Network Profiles > IKE Crypto*

Use the **IKE Crypto Profiles** page to specify protocols and algorithms for identification, authentication, and encryption in VPN tunnels based on IPSec SA negotiation (IKEv1 Phase-1).

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

Table 196. IKE Crypto Profile Settings

Field	Description
DH Group	Specify the priority for Diffie-Hellman (DH) groups. Click Add and select groups. For highest security, select an item and then click the Move Up or Move Down icon to move the groups with higher numeric identifiers to the top of the list. For example, move group14 above group2 .
Authentication	Specify the priority for hash algorithms. Click Add and select algorithms (md5, sha1, sha256, sha384, or sha512). For highest security, use the arrows to move sha1 to the top of the list.
Encryption	Select the check boxes for the desired Encapsulating Security Payload (ESP) authentication options. Click Add and select algorithms (aes256, aes192, aes128, or 3des). For highest security, select an item and then click the Move Up or Move Down icon to change the order to the following: aes256, aes192, aes128, 3des .
Lifetime	Select units and enter the length of time that the negotiated key will stay effective.

Defining IPSec Crypto Profiles

► *Network > Network Profiles > IPSec Crypto*

Use the **IPSec Crypto Profiles** page to specify protocols and algorithms for identification, authentication, and encryption in VPN tunnels based on IPSec SA negotiation (IKEv1 Phase-2).

Table 197. IPSec Crypto Profile Settings

Field	Description
Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
IPSec Protocol	<p>Choose an option from the drop-down list.</p> <p>ESP:</p> <ul style="list-style-type: none"> Click Add under Encryption and select the desired ESP encryption algorithms. For highest security, use the arrows to change the order to the following: 3des, aes128, aes192, aes256, or aes128ccm16. Click Add under Authentication and select the desired ESP authentication algorithms (md5, sha1, sha256, sha384, sha512, or none). <p>AH:</p> <ul style="list-style-type: none"> Click Add under Authentication and select the desired AH authentication algorithms (md5, sha1, sha256, sha384, or sha512).
DH Group	Select the DH group. For highest security, choose the group with the highest identifier.
Lifetime	Select units and enter the length of time that the negotiated key will stay effective. The default is 1 hour.
Lifesize	Select optional units and enter the amount of data that the key can use for encryption.

To change the ordering in which an algorithm or group is listed, select an item and then click the Move Up or Move Down icon to change the order. The listed order determines the order in which the algorithms are applied and can affect tunnel performance.

Chapter 9

GlobalProtect Settings

Setting Up the GlobalProtect Portal

► *Network > GlobalProtect > Portals*

Use this page to set up and manage a GlobalProtect portal configuration. The portal provides the management functions for the GlobalProtect infrastructure. Every client system that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the gateways. In addition, the portal controls the behavior and distribution of the GlobalProtect agent software to both Mac and Windows laptops. (On mobile devices, the GlobalProtect app is distributed through the Apple App Store for iOS devices or through Google Play for Android devices.)

To add a portal configuration, click **Add** to open the GlobalProtect Portal dialog. For detailed information on the fields on each tab of the dialog, see the following sections:

- “[Portal Configuration Tab](#)”
- “[Client Configuration Tab](#)”
- “[Satellite Configuration Tab](#)”

For detailed step-by-step instructions on setting up the portal, see “Configure a GlobalProtect Portal” in the [GlobalProtect Administrator’s Guide](#).

Portal Configuration Tab

Use the **Portal Configuration** tab to define the network settings to enable agents to connect to the portal and specify how the portal will authenticate end clients.

In addition, you can use this tab to optionally specify custom GlobalProtect portal login and help pages. For information on how to create and import these custom pages, see “Customize the Portal Login, Welcome, and Help Pages” in the [GlobalProtect Administrator’s Guide](#).

Table 198. GlobalProtect Portal Settings

Field	Description
Name	Enter a name for the portal (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in Multiple Virtual System Mode, the Location is the virtual system (vsys) where the GlobalProtect portal is available. For a firewall that is not in Multiple Virtual System Mode, the Location field does not appear in the GlobalProtect Portal dialog. After you save the portal, you cannot change its Location .
Network Settings	
Interface	Select the firewall interface that will be used as the ingress for remote clients/firewalls.
IP Address	Specify the IP address on which GlobalProtect portal web service will be running.
Server Certificate	Select the SSL server certificate to use for the GlobalProtect portal. The Common Name (CN) and, if applicable, the Subject Alternative Name (SAN) fields of the certificate must exactly match the IP address or fully qualified domain name (FQDN) of the interface you selected. As a best practice in GlobalProtect VPN configurations, use a certificate from a trusted third-party CA or a certificate generated by your internal Enterprise CA. If you have not yet generated/imported the server certificate you can Generate it now (if you have already created a root CA certificate for self-signing), or you can Import a certificate from an external CA.
Authentication	
Authentication Profile	Choose an authentication profile to authenticate clients/satellites accessing the portal. If you are configuring LVPN, you will not be able to save the configuration unless you select an authentication profile. Even if you plan to authenticate satellites using serial numbers, the portal requires an authentication profile to fall back to if it cannot locate or validate the serial number. See " Setting Up Authentication Profiles ".
Authentication Message	Enter a message to help end users know what credentials they should use for logging in to the portal or use the default message. The message can be up to 50 characters in length.
Client Certificate	(Optional) If you plan to use mutual SSL authentication, select the certificate the client will present to the gateways. This client certificate will be distributed to all agents that successfully authenticated to the portal unless the corresponding client configuration for the agent contains a different client certificate. If you are using an internal CA to distribute certificates to clients, leave this field blank.
Certificate Profile	(Optional) Select the certificate profile to use to authenticate users on the portal. Only use this option if the end points will already have a client certificate pre-deployed using your internal public key infrastructure (PKI).
Appearance	

Table 198. GlobalProtect Portal Settings (Continued)

Field	Description
Disable login page	Select this option to disable access to the GlobalProtect portal login page from a web browser.
Custom Login Page	Choose an optional custom login page for user access to the portal.
Custom Help Page	Choose an optional custom help page to assist the user with GlobalProtect.

Client Configuration Tab

Use the **Client Configuration** tab to define the GlobalProtect client configuration settings that the portal will deploy to the agent/app upon successfully connecting and authenticating.

(Optional, but highly recommended) This tab also allows you to automatically deploy any **Trusted Root CA** certificates and intermediate certificates the end clients will need in order to establish HTTPS connections with the GlobalProtect gateways and/or the GlobalProtect Mobile Security Manager. Any certificates you add here will be pushed to the clients with the client configuration. If you do not deploy a trusted root CA certificate in the client configuration, the agent will not check the validity of the gateway certificate when connecting to the gateway. Therefore, as a best practice for preventing man-in-the-middle attacks, you should always deploy the trusted Root CA certificate of the gateway in the client configuration. To add a **Trusted Root CA** certificate, click **Add** and then select a certificate from the list or click **Import** to browse for and import the certificate onto the firewall.

If you have different classes of users requiring different configurations, you can create a separate client configuration for each. The portal will then use the username/group name and or OS of the client to determine which client configuration to deploy. As with security rule evaluation, the portal looks for a match starting from the top of the list. When it finds a match, it delivers the corresponding configuration to the agent/app. Therefore, if you have multiple client configurations it is important to order them so that more specific configurations (that is configurations for specific users or operating systems) are above more generic configurations. Use the **Move Up** and **Move Down** buttons to order the configurations. Click **Add** to open the **Configs** dialog and create a new client configuration. For detailed information on configuring the portal and creating a client configurations, see “Configure the GlobalProtect Portal” in the *GlobalProtect Administrator’s Guide*.

The **Configs** dialog contains five tabs, which are described in the following table:

- [General tab](#)
- [User/User Group tab](#)
- [Gateways tab](#)
- [Agent tab](#)
- [Data Collection tab](#)

Table 199. GlobalProtect Portal Client Configuration Settings

Field	Description
General Tab	
Name	Enter a name to identify this client configuration.

Table 199. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Use single sign-on	Select the check box to have GlobalProtect use the users' Windows login credentials to transparently connect and authenticate to the GlobalProtect portal and gateways. Users will not be required to enter a username and password in the agent Settings tab.
Config Refresh Interval (hours)	Specify the interval in hours at which to refresh the GlobalProtect agent configuration (default 24 hours; range 1-168 hours).
Authentication Modifier	<ul style="list-style-type: none"> • None—The portal always authenticates the agent using the specified authentication profile and/or certificate profile and sends the authentication credentials to the gateway. This is the default setting. • Cookie authentication for config refresh—Allow cookie-based agent authentication to the portal for refreshing a cached client configuration. • Cookie Expire (days)—This option displays only if you select Cookie authentication for config refresh from the Authentication Modifier field. Use it to specify the number of days that the agent can use the cookie to authenticate to the portal for a configuration refresh; a value of 0 (the default) indicates that the cookie never expires. • Different password for external gateway—Indicates that the portal and the gateway use different authentication credentials and prompts the user for gateway password after portal authentication succeeds. By default, the portal will send the same password the agent used to authenticate to the portal on to the gateway. • Manual Gateway Only—This option displays only if you select Different password for external gateway from the Authentication Modifier field. Select this check box if you want to be able to use different authentication mechanisms on different gateways that are configured as Manual gateways. For example, you might choose to use Active Directory credentials for an "always on" connection to one set of gateways, and use a stronger authentication mechanism, such as a two-factor OTP authentication on another set of gateways protecting more secure resources.
Connect Method	<ul style="list-style-type: none"> • on-demand—Select this option to allow users to establish a connection on demand. With this option, the user must explicitly initiate the connection. This function is primarily used for remote access connections. • user-logon—When this option is set, the GlobalProtect agent will automatically establish a connection after users log in to their computers. If you select Use single sign-on, the username and password used to log in to Windows is captured by the GlobalProtect agent and used to authenticate. • pre-logon—Allows the agent to authenticate and establish the VPN tunnel to the GlobalProtect gateway using a pre-installed machine certificate before the user has logged in to the machine. When using the pre-logon connect method, you can create GlobalProtect client configurations and security policies that specify pre-logon as the source user and enable access only to basic services, such as DHCP, DNS, Active Directory, and antivirus and operating system update services, to further speed up the login process for users. To use this feature, you must use your own public-key infrastructure (PKI) to issue and distribute certificates to your end-user systems. You must then import the root CA certificate used to issue the machine certificates onto the firewall (both the portal and the gateway) and then create a corresponding certificate profile.

Table 199. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Client Certificate	If you want to use mutual SSL authentication, select the certificate the client will present to the gateways. This client certificate will be distributed to all agents that match this client configuration. If there is also a client certificate specified on the Portal Configuration tab, this one will be used instead. If you are deploying unique certificates to your end points using an internal PKI, leave this field blank.
Mobile Security Manager	If you are using the GlobalProtect Mobile Security Manager for mobile device management, enter the IP address or FQDN of the device check-in/enrollment interface on the GP-100 appliance.
Enrollment Port	The port number the mobile device should use when connecting to the GlobalProtect Mobile Security Manager for enrollment. By default, the Mobile Security Manager listens on port 443 and it is a best practice to leave it set to this value so that mobile device users are not prompted for a client certificate during the enrollment process. (Default: 443; Possible values: 443, 7443, 8443)
Internal Host Detection	<p>With this option, GlobalProtect does a reverse DNS lookup of the specified Hostname to the specified IP Address. If it does not match, GlobalProtect determines the end point is outside of the corporate network and establishes a tunnel with any of the available external gateways configured in the Gateways tab. If it matches, the agent determines that the end point is inside the network and connects to an internal gateway (if configured); it does not create a VPN connection to any external gateways in this case.</p> <p>Select the check box to enable internal host detection using DNS lookup. Specify the following:</p> <ul style="list-style-type: none"> • IP Address—Enter an internal IP address for the internal host detection. • Hostname—Enter the hostname that resolves to the above IP address within the internal network.

User/User Group Tab

Specify the user or user group to and/or client operating system to which to apply the client configuration:

- **User/User Group**—Click **Add** to select a specific user or user group to which this configuration will apply from the list (group mapping must be configured for the list of users and groups to display). You can also create configurations to be deployed to agents in **pre-logon** mode (that is, before the user has logged in to the system), or configurations to be applied to **any** user.
- **OS**—To deploy configurations based on the specific operating system running on the end system, click **Add** in the OS section of the Window and then select the applicable operating systems (**Android**, **iOS**, **Mac**, or **Windows**). Or leave the value in this section set to **Any** for the configurations to be deployed based on user/group only.

Gateways Tab

Cutoff Time	Specify the amount of time (in seconds) the agent will wait for gateways to respond before determining the best gateway to connect to. The agent will then attempt to connect to only those gateways that responded within the specified Cutoff Time. The default value is 5. A value of 0 indicates that there is no cutoff time; the agent will wait until the TCP timeout. (Range 0 to 10)
-------------	---

Table 199. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Internal Gateways	Specify the internal firewalls that the agent will authenticate and provide HIP reports to.
External Gateways	Specify the list of firewalls the agent should try to establish a tunnel with when not on the corporate network. Click Add and then enter the following information for each external gateway: <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 connect to. The agent will contact all of the gateways (except those with a priority of Manual only) and establish a tunnel with the firewall that provides the fastest response and the highest Priority value. • Manual—Select this check box if you want to allow users to manually connect to (or switch to) the gateway. The GlobalProtect agent will have the option to connect to any external gateway that is configured as Manual selection. When connecting to the new gateway, the existing tunnel will be disconnected and a new tunnel will be established. The manual gateways can also have different authentication mechanism than the primary gateway. If the client system is restarted, or if a rediscovery is performed, the GlobalProtect agent will connect to the primary gateway. This feature is useful if you have a group of users who need to temporarily connect to a specific gateway to access a secure segment of your network.
Agent Tab	The settings on this tab specify how end users interact with the GlobalProtect agents installed on their systems. You can define different agent settings for the different GlobalProtect client configurations you create.
Passcode/Confirm Passcode	Enter the passcode that end users will need to enter to override the agent. This field is only required if the Agent User Override field is set to without passcode.

Table 199. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Agent User Override	<p>Select an override option:</p> <ul style="list-style-type: none"> • disabled—Prevents end users from disabling the GlobalProtect agent. • with-comment—Prompts the end user to enter a comment when disabling the GlobalProtect agent. • with-passcode—The option allows the user to enter a passcode to override the GlobalProtect agent. If you select this option, you must also enter a value in the Passcode and Confirm Passcode field. Users will have to enter this value in order to override the agent. • with-ticket—This option enables a challenge-response mechanism to authorize disabling GlobalProtect agent on the client side. When this option is selected, the user is prompted with a challenge when disabling GlobalProtect. The challenge is then communicated to the firewall administrator out-of-band, and the administrator can validate the challenge through the firewall management interface. The firewall produces a response that is read back to the user who can then disable GlobalProtect by entering the response when prompted by the GlobalProtect agent. When using this option, you must also enter the key for decrypting the ticket in the Agent User Override Key fields at the top-level of the Client Configuration tab.
Max Times User Can Disable	<p>Specify the maximum number of times a user can disable GlobalProtect before a successful connection to a firewall is required. A value of 0 (the default) indicates that agent overrides are unlimited.</p>
User Can Disable Timeout (min)	<p>Specify the maximum length of time (in minutes) that GlobalProtect will be disabled upon override; after the specified amount of time elapses, the agent will reconnect. A value of 0 (the default) indicates that the duration of the override is unlimited.</p>
Agent Upgrade	<p>Select one of the following options to specify how GlobalProtect agent software downloads/upgrades will occur:</p> <ul style="list-style-type: none"> • disabled—Prevents users from upgrading the agent. • manual—Allow users to manually check for and initiate upgrades by selecting the agent Check Version option. • prompt—Prompt end users to upgrade whenever a new agent version is activated on the firewall. This is the default setting. • transparent—Automatically upgrade the agent software whenever a new version is available on the portal.
Welcome Page	<p>Select a welcome page to display to end users upon successfully connecting to GlobalProtect. You can select the factory-default page or Import a custom page. By default this field is set to None.</p>
Third Party VPN	<p>Click Add to add a list of third-party remote access VPN clients that might be present on the end points. If configured, GlobalProtect will ignore those VPN clients and their route settings to ensure that it does not interfere or conflict with them.</p>
Enable advanced view	<p>Deselect this check box to restrict the user interface on the client side to the basic minimum view. By default, the advanced view setting is enabled.</p>

Table 199. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Show GlobalProtect icon	Clear this check box to hide the GlobalProtect icon on the client system. When hidden, users cannot perform other tasks such as changing passwords, rediscovering the network, resubmitting host information, viewing troubleshooting information, or performing an on-demand connection. However, HIP notification messages, login prompts, and certificate dialogs will still display as necessary for interacting with the end user.
Allow user to change portal address	Clear this check box disable the Portal field on the Settings tab in the GlobalProtect agent. Because the user will then be unable to specify a portal to which to connect, you must supply the default portal address in the Windows Registry: (HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup with key Portal) or the Mac plist (/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist with key Portal).
Allow user to save password	Clear this check box to prevent users from saving their passwords on the agent (that is, you want to force them to provide the password—either transparently via the client or by manually entering one—each time they connect).
Enable Rediscover Network option	Clear this check box to prevent users from performing a manual network rediscovery.
Enable Resubmit Host Profile option	Clear this check box to prevent users from manually triggering resubmission of the latest HIP.
Allow user to continue if portal server certificate is invalid	Clear this check box to prevent the agent from establishing a connection with the portal if the portal certificate is not valid.
Data Collection Tab	
Use this subtab to define what data the agent will collect from the client in the HIP report:	
Max Wait Time	Specify how long the agent should search for the HIP data before submitting the information available (range 10-60 seconds; default 20 seconds).
Exclude Categories	Use this subtab to define any host information categories for which you do not want to collect HIP data. Select a Category to exclude from HIP collection. After selecting a category, optionally refine the exclusion by clicking Add and then selecting the particular Vendor . Click Add in the Product section of the dialog and then select the products from the vendor. Click OK to save settings.

Table 199. GlobalProtect Portal Client Configuration Settings (Continued)

Field	Description
Custom Checks	<p>Use this subtab to define any custom host information that you want the agent to collect. For example, if you have any required applications that are not included in the Vendor and/or Product lists for creating HIP objects, create a custom check that will allow you to determine whether that application is installed (has a corresponding registry or plist key) or is running (has a corresponding running process):</p> <ul style="list-style-type: none"> • Windows—Click Add to add a check for a particular registry key and/or key value. • Mac—Click Add to add a check for particular plist key or key value. • Process List—Click Add to specify the list of processes to be checked on the end user systems to see if they are running. For example, to determine whether a software application is running, add the name of the executable file to the process list. You can add a Process List to the Windows tab or the Mac tab.

Satellite Configuration Tab

A satellite device is a Palo Alto Networks firewall—typically at a branch office—that acts as a GlobalProtect agent to enable it to establish VPN connectivity to a GlobalProtect gateway. Like a GlobalProtect agent, the satellite receives its initial configuration from the portal, which includes the certificates and VPN configuration routing information to enable it to connect to all configured gateways to establish VPN connectivity.

Before configuring the GlobalProtect satellite settings on the branch office firewall, you must first configure an interface with WAN connectivity and set up a security zone and policy to allow the branch office LAN to communicate with the Internet. You can then configure the GlobalProtect satellite settings on the portal as described in the following table:

Table 200. GlobalProtect Portal Satellite Configuration Settings

Field	Description
General subtab	<p>Click Add to display the subtabs, and specify the following on the GlobalProtect Satellite > General subtab:</p> <ul style="list-style-type: none"> • Name—Enter a name to identify the GlobalProtect satellite device profile. • Configuration Refresh Interval (hours)—Specify how often satellite devices should check the portal for configuration updates (default 24 hours, range 1-48 hours).
Devices subtab	<p>Click Add to manually add a satellite device using the device serial number. If you use this option, when the satellite device first connects to receive the authentication certificate and the initial configuration, no user login prompt is required. After the satellite device authenticates, the Name (host name) will be added automatically to the Portal.</p>

Table 200. GlobalProtect Portal Satellite Configuration Settings (Continued)

Field	Description
Enrollment User/User Group subtab	<p>The portal uses the Enrollment User/User Group settings and/or Devices serial numbers to match a satellite to a configuration.</p> <p>Specify the match criteria for the satellite configuration as follows:</p> <ul style="list-style-type: none"> To restrict this configuration to satellite devices with specific serial numbers, select the Devices tab, click Add, and enter serial number (you do not need to enter the satellite hostname; it will be automatically added when the satellite connects). Repeat this step for each satellite you want to receive this configuration. Select the Enrollment User/User Group tab, click Add, and then select the user or group you want to receive this configuration. Satellites that do not match on serial number will be required to authenticate as a user specified here (either an individual user or group member). <p>Note: Note Before you can restrict the configuration to specific groups, you must enable Group Mapping.</p>
Gateways subtab	<p>Click Add to enter the IP address or hostname of the gateway(s) satellites with this configuration can establish IPSec tunnels with. Enter the FQDN or IP address of the interface where the gateway is configured in the Gateways field</p> <p>(Optional) If you are adding two or more gateways to the configuration, the Routing Priority helps the satellite pick the preferred gateway. Enter a value in the range of 1-25, with lower numbers having the higher priority (that is, the gateway the satellite will connect to if all gateways are available). The satellite will multiply the routing priority by 10 to determine the routing metric.</p> <p>Note: Routes published by the gateway are installed on the satellite as static routes. The metric for the static route is 10x the routing priority. If you have more than one gateway, make sure to also set the routing priority to ensure that routes advertised by backup gateways have higher metrics compared to the same routes advertised by primary gateways. For example, if you set the routing priority for the primary gateway and backup gateway to 1 and 10 respectively, the satellite will use 10 as the metric for the primary gateway and 100 as the metric for the backup gateway.</p> <p>The satellite will also share its network and routing information with the gateways if the Publish all static and connected routes to Gateway (configured on the satellite in Network > IPSec tunnels > Advanced tab) option is selected. See “GlobalProtect Satellite” for more details.</p>
Trusted Root CA	<p>Click Add and then select the CA certificate used to issue the gateway server certificates. As a best practice, all of your gateways should use the same issuer.</p> <p>Note: If the root CA certificate used to issue your gateway server certificates is not on the portal, you can Import it now.</p>
Issuing Certificate	Select the Root CA certificate that for the portal to use to issue certificates to satellites upon successfully authenticating them.
Validity Period (days)	Specify the issued GlobalProtect satellite certificate lifetime (default 7 days, range 7-365 days).

Table 200. GlobalProtect Portal Satellite Configuration Settings (Continued)

Field	Description
Certificate Renewal Period (days)	Specify the GlobalProtect satellite certificate renewal period (default 3 days, range 3-30 days). This will determine how often certificates should be renewed.
OCSP Responder	Select the OCSP responder for the satellites to use to verify the revocation status of certificates presented by the portal and gateways.

Setting Up the GlobalProtect Gateways

► *Network > GlobalProtect > Gateways*

Use this page to configure a GlobalProtect gateway. The gateway can be used to provide VPN connections for GlobalProtect agents/apps or GlobalProtect satellite devices.

To add a gateway configuration, click **Add** to open the GlobalProtect Portal dialog. For detailed information on the fields on each tab of the dialog, see the following sections:

- “General Tab”
- “Client Configuration Tab”
- “Satellite Configuration Tab”

For detailed step-by-step instructions on setting up a gateway, see “Configure a GlobalProtect Gateway” in the *GlobalProtect Administrator’s Guide*.

General Tab

Use the **General** tab to define the gateway interface to which agents/apps will connect and specify how the gateway will authenticate end clients.

Table 201. GlobalProtect Gateway General Settings

Field	Description
Name	Enter a name for the gateway (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in Multiple Virtual System Mode, the Location is the virtual system (vsys) where the GlobalProtect gateway is available. For a firewall that is not in Multiple Virtual System Mode, the Location field does not appear in the GlobalProtect Gateway dialog. After you save the gateway, you cannot change its Location .

Network Settings

Interface	Select the firewall interface that will be used as the ingress for remote agents/satellites.
IP Address	Specify the IP address for gateway access.
Server Certificate	Choose the server certificate for the gateway.

Authentication

Table 201. GlobalProtect Gateway General Settings (Continued)

Field	Description
Authentication Profile	Choose an authentication profile or sequence to authenticate access to the gateway. See “ Setting Up Authentication Profiles ”.
Authentication Message	Enter a message to help end users know what credentials they should use for logging in to this gateway or use the default message. The message can be up to 50 characters in length.
Certificate Profile	Choose the certificate profile for client authentication.

Client Configuration Tab

Use the Client Configuration tab to configure the tunnel settings to enable agents/apps to establish VPN tunnels with the gateway. In addition, use this tab to define HIP notification messages to display to end users upon matching/not matching a HIP profile attached to a security policy.

This tab contains the three subtabs, which are described in the following table:

- [Tunnel Settings subtab](#)
- [Network Settings subtab](#)
- [HIP Notification subtab](#)

Table 202. GlobalProtect Gateway Client Configuration Settings

Field	Description
Tunnel Settings subtab	<p>Use this subtab to configure the tunnel parameters and enable tunneling. The tunnel parameters are required if you are setting up an external gateway. If you are configuring an internal gateway, they are optional.</p>
Tunnel Mode	<p>Select the check box to enable tunnel mode and specify the following settings:</p> <ul style="list-style-type: none"> • Tunnel Interface—Choose the tunnel interface for access to the gateway. • Max User—Specify the maximum number of users that can access the gateway at the same time for authentication, HIP updates, and GlobalProtect agent updates. If the maximum number of users is reached, subsequent users are denied access with an error message indicating that the maximum number of users has been reached. By default, there is no limit set (range=1-1024 users). • Enable IPSec—Select the check box to enable IPSec mode for client traffic, making IPSec the primary and SSL-VPN the fall back method. • Enable X-Auth Support—Select the check box to enable Extended Authentication (X-Auth) support in the GlobalProtect gateway when IPSec is enabled. With X-Auth support, third party IPSec VPN clients that support X-Auth (such as the IPSec VPN client on Apple iOS and Android devices and the VPNC client on Linux) can establish a VPN tunnel with the GlobalProtect gateway. The X-Auth option provides remote access from the VPN client to a specific GlobalProtect gateway. Because X-Auth access provides limited GlobalProtect functionality, consider using the GlobalProtect App for simplified access to the full security feature set GlobalProtect provides on iOS and Android devices. <p>Selecting the X-Auth Support check box enables 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 user name and password, which is verified through the authentication profile configured in the Authentication section. – If no group name and group password are defined, the first authentication phase is based on a valid certificate presented by the third-party VPN client. This certificate is then validated through the certificate profile configured in the authentication section. – By default, the user is not required to re-authenticate when the key used to establish the IPSec tunnel expires. To require the user to re-authenticate, clear the Skip Auth on IKE Rekey check box.
Timeout Configuration	<p>Specify the following timeout settings:</p> <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 given amount of time.

Table 202. GlobalProtect Gateway Client Configuration Settings (Continued)

Field	Description
Network Settings subtab	The Network Settings options are available only if you have enabled Tunnel Mode and defined a Tunnel Interface on the Tunnel Settings tab. The network settings defined here will be assigned to the virtual network adapter on the client system when an agent establishes a tunnel with the gateway.
Inheritance Source	Select a source to propagate DNS server and other settings from the selected DHCP client or PPPoE client interface into the GlobalProtect agents' configuration. With this setting all client network configuration, such as DNS servers and WINS servers, are inherited from the configuration of the interface selected in the Inheritance Source.
Check inheritance source status	Click the link to see the server settings that are currently assigned to the client interfaces.
Primary DNS Secondary DNS	Enter the IP addresses of the primary and secondary servers that provide DNS to the clients.
Primary WINS Secondary WINS	Enter the IP addresses of the primary and secondary servers that provide Windows Internet Naming Service (WINS) to the clients.
DNS Suffix	Click Add to enter a suffix that the client should use locally when an unqualified hostname is entered that it cannot resolve. You can enter multiple suffixes by separating them with commas.
Inherit DNS Suffixes	Select this check box to inherit the DNS suffixes from the inheritance source.
IP Pool	Click Add to specify IP pool settings. Use this section to create a range of IP addresses to assign to remote users. When the tunnel is established, an interface is created on the remote user's computer with an address in this range. <i>Note: The IP pool must be large enough to support all concurrent connections. IP address assignment is dynamic and not retained after the user disconnects. Configuring multiple ranges from different subnets will allow the system to offer clients an IP address that does not conflict with other interfaces on the client.</i> The servers/routers in the networks must route the traffic for this IP pool to the firewall. For example, for the 192.168.0.0/16 network, a remote user may be assigned the address 192.168.0.10.
Access Route	Click Add to specify access route options. Use this section to add routes that will be pushed to the remote user's computer and therefore determine what the user's computer will send through the VPN connection. For example, you can set up split tunneling to allow remote users to access the Internet without going through the VPN tunnel. If no route is added, then every request is routed through the tunnel (no split tunneling). In this case, each Internet request passes through the firewall and then out to the network. This method can prevent the possibility of an external party accessing the user's computer and then gaining access to the internal network (with the user's computer acting as bridge).

Table 202. GlobalProtect Gateway Client Configuration Settings (Continued)

Field	Description
HIP Notification subtab	<p>Use this subtab to define the notification messages end users will see when a security rule with a host information profile (HIP) is enforced. This step only applies if you have created host information profiles and added them to your security policies.</p>
HIP Notification	<p>Click Add to specify notification options. Select Enable to enable the Match Message and/or Not Match Message.</p> <p>Choose a notification option from the Show Notification As section and choose the radio button for a System Tray Balloon or Pop Up Message, and then specify a message to match or not match. Use these settings to notify the end user about the state of the machine, for example, to provide a warning message that the host system does not have a required application installed. For the Match Message, you can also enable the option to Include Mobile App List to indicate what applications triggered the HIP match.</p> <p><i>Note:</i> The HIP notification messages can be formatted in rich HTML, which can include links to external web sites and resources. Use the link icon  in the rich text settings toolbar to add links.</p>

Satellite Configuration Tab

A satellite device is a Palo Alto Networks firewall—typically at a branch office—that acts as a GlobalProtect agent to enable it to establish VPN connectivity to a GlobalProtect gateway. Use the **Satellite Configuration** tab to define the gateway tunnel and network settings to enable the satellite devices to establish VPN connections with it. You can also use this tab to control the routes advertised by the satellites.

This tab contains the three subtabs, which are described in the following table:

- [Tunnel Settings subtab](#)
- [Network Settings subtab](#)
- [Route Filter subtab](#)

Table 203. GlobalProtect Gateway Satellite Configuration Settings

Field	Description
Tunnel Settings subtab	<p>Tunnel Configuration—Select the Tunnel Configuration check box and select an existing Tunnel Interface, or click New Tunnel Interface. See “Configuring a Tunnel Interface” for more information.</p> <p>Replay attack detection—Protect against replay attacks.</p> <p>Copy TOS—Copy the (Type of Service) ToS header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original ToS information.</p> <p>Configuration refresh interval (hours)—Specify how often satellite devices should check the portal for configuration updates (default 2 hours; range 1-48 hours).</p>

Table 203. GlobalProtect Gateway Satellite Configuration Settings (Continued)

Field	Description
Tunnel Monitoring	Select the Tunnel Monitoring check box to enable the satellite devices to monitor gateway tunnel connections, allowing them to failover to a backup gateway if the connection fails. Destination IP —Specify an IP address for the tunnel monitor will use to determine if there is connectivity to the gateway (for example, an IP address on the network protected by the gateway). Alternatively, if you configured an IP address for the tunnel interface, you can leave this field blank and the tunnel monitor will instead use the tunnel interface to determine if the connection is active. Tunnel Monitor Profile—Failover to another gateway is the only type of tunnel monitoring profile supported with LVPN.
Crypto Profiles	Select an IPSec Crypto Profile , or create a new profile. This will determine the protocols and algorithms for identification, authentication, and encryption for the VPN tunnels. Because both tunnel endpoints in an LVPN are trusted firewalls within your organization, you can typically use the default profile, which uses ESP-DH group2-AES 128 with SHA-1 encryption. See “ Defining IPSec Crypto Profiles ” for more details.
Network Settings subtab	
Inheritance Source	Select a source to propagate DNS server and other settings from the selected DHCP client or PPPoE client interface into the GlobalProtect satellite configuration. With this setting all network configuration, such as DNS servers, are inherited from the configuration of the interface selected in the Inheritance Source.
Primary DNS Secondary DNS	Enter the IP addresses of the primary and secondary servers that provide DNS to the satellites.
DNS Suffix	Click Add to enter a suffix that the satellite should use locally when an unqualified hostname is entered that it cannot resolve. You can enter multiple suffixes by separating them with commas.
Inherit DNS Suffix	Select this check box to send the DNS suffix to the satellite devices to use locally when an unqualified hostname is entered that it cannot resolve.
IP Pool	Click Add to specify IP pool settings. Use this section to create a range of IP addresses to assign to the tunnel interface on satellite devices upon establishment of the VPN tunnel. <i>Note:</i> The IP pool must be large enough to support all concurrent connections. IP address assignment is dynamic and not retained after the satellite disconnects. Configuring multiple ranges from different subnets will allow the system to offer satellites an IP address that does not conflict with other interfaces on the device. The servers/routers in the networks must route the traffic for this IP pool to the firewall. For example, for the 192.168.0.0/16 network, a satellite may be assigned the address 192.168.0.10. If you are using dynamic routing, make sure that the IP address pool you designate for satellites does not overlap with the IP addresses you manually assigned to the tunnel interfaces on your gateways and satellites.

Table 203. GlobalProtect Gateway Satellite Configuration Settings (Continued)

Field	Description
Access Route	click Add and then enter the routes as follows: <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 will route traffic that is not destined for a specified access route using its own routing table. For example, you may choose to only tunnel traffic destined for your corporate network, and use the local satellite to safely enable Internet access. • If you want to enable routing between satellites, enter the summary route for the network protected by each satellite.
Route Filter subtab	Select the Accept published routes check box to accept routes advertised by the satellite into the gateway's routing table. If you do not select this option, the gateway will not accept any routes advertised by the satellites. If you want to be more restrictive on accepting the routes advertised by the satellites, click Add in the Permitted subnets section to define the subnets for which the gateway should accept routes; subnets advertised by the satellites that are not part of the list will be filtered out. For example, if all the satellites are configured with 192.168.x.0/24 subnet on the LAN side, you can configure a permitted route of 192.168.0.0/16 on the gateway. This will result in the gateway accepting the routes from the satellite only if it is in the 192.168.0.0/16 subnet.

Setting Up Gateway Access to a Mobile Security Manager

► *Network > GlobalProtect > MDM*

If you are using a Mobile Security Manager to manage end user mobile devices and you are using HIP-enabled policy enforcement, you must configure the gateway to communicate with the Mobile Security Manager to retrieve the HIP reports for the managed devices. Use this page to enable the gateway to access the Mobile Security Manager.

To add information for a Mobile Security Manager, click **Add**. The following table provides information on what to enter in the fields on the GlobalProtect MDM dialog. For more detailed information on setting up the GlobalProtect Mobile Security Manager service, see "Set Up the GlobalProtect Mobile Device Manager" in the *GlobalProtect Administrator's Guide*.

For detailed step-by-step instructions for setting up the gateway to retrieve the HIP reports on the GlobalProtect Mobile Security Manager, see “Enable Gateway Access to the GlobalProtect Mobile Security Manager.”

Table 204. GlobalProtect MDM Settings

Field	Description
Name	Enter a name for the Mobile Security Manager (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Location	For a firewall that is in Multiple Virtual System Mode, the Location is the virtual system (vsys) where the Mobile Security Manager is available. For a firewall that is not in Multiple Virtual System Mode, the Location field does not appear in the MDM dialog. After you save the Mobile Security Manager, you cannot change its Location .
Connection Settings	
Server	Enter the IP address or FQDN of the interface on the Mobile Security Manager where the gateway will connect to retrieve HIP reports. Ensure that you have a service route to this interface.
Connection Port	The port the Mobile Security Manager will listen on for HIP report requests. The default port is 5008, which is the port that the GlobalProtect Mobile Security Manager listens on. If you are using a third-party Mobile Security Manager, enter the port number on which that server listens for HIP report requests.
Client Certificate	Choose the client certificate for the gateway to present to the Mobile Security Manager when establishing an HTTPS connection. This is only required if the Mobile Security Manager is configured to use mutual authentication.
Trusted Root CA	Click Add and select the root CA certificate that was used to issue the certificate for the interface where the gateway will connect to retrieve HIP reports (this could be a different server certificate than the one issued for the device check-in interface on the Mobile Security Manager). You must import the root CA certificate and add it to this list.

Creating HIP Objects

► *Objects > GlobalProtect > HIP Objects*

Use this page to define host information profile (HIP) objects. HIP objects provide the matching criteria to filter out the host information you are interested in using to enforce policy from the raw data reported by the agent/app. For example, while the raw host data may include information about several antivirus packages that are installed on the client, you may only be interested in one particular application that you require within your organization. In this case, you would create a HIP object to match the specific application you are interested in enforcing.

The best way to determine what HIP objects you need is to determine how you will use the host information you collect to enforce policy. Keep in mind that the HIP objects themselves are merely building blocks that allow you to create the HIP profiles that are used in your security policies. Therefore, you may want to keep your objects simple, matching on one thing, such as the presence of a particular type of required software, membership in a specific domain, or the presence of a specific client OS. By doing this, you will have the flexibility to create a very granular HIP-augmented policy.

To create a HIP object, click **Add** to open the HIP Object dialog. For a description of what to enter in a specific field, see the following tables.

- “General Tab”
- “Mobile Device Tab”
- “Patch Management Tab”
- “Firewall Tab”
- “Antivirus Tab”
- “Anti-Spyware Tab”
- “Disk Backup Tab”
- “Disk Encryption Tab”
- “Data Loss Prevention Tab”
- “Custom Checks Tab”

For more detailed information on creating HIP-augmented security policies, see “Configure HIP-Based Policy Enforcement” in the *GlobalProtect Administrator’s Guide*.

General Tab

Use the **General** tab to specify a name for the new HIP object and to configure the object to match against general host information such as domain, operating system, or the type of network connectivity it has.

Table 205. HIP Object General Settings

Field	Description
Name	Enter a name for the HIP object (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Shared	<p>Select this check box if you want the HIP object to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the object will be available only to the vsys selected in the Virtual System drop-down (Objects > GlobalProtect > HIP Objects page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the HIP Object dialog. • All device groups on Panorama. If you clear the check box, the object will be available only to the device group selected in the Device Group drop-down (Objects > GlobalProtect > HIP Objects page). <p>After you save the object, you cannot change its Shared setting. The Objects > GlobalProtect > HIP Objects page shows the current setting in the Location field.</p>
Description	Enter an optional description.
Host Info	Select the check box to enable filtering on the host information fields.
Domain	To match on a domain name, choose an operator from the drop-down list and enter a string to match.
OS	To match on a host OS, choose Contains from the first drop-down, select a vendor from the second drop-down, and then select a specific OS version from the third drop-down, or select All to match on any OS version from the selected vendor.
Client Versions	To match on a specific version number, select an operator from the drop-down and then enter a string to match (or not match) in the text box.
Host Name	To match on a specific host name or part of a host name, select an operator from the drop-down and then enter a string to match (or not match, depending on what operator you selected) in the text box.
Network	<p>Use this field to enable filtering on a specific mobile device network configuration. This match criteria applies to mobile devices only.</p> <p>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.</p>

Mobile Device Tab

Use the **Mobile Device** tab to enable HIP matching on data collected from mobile devices running the GlobalProtect app.

Table 206. HIP Object Mobile Device Settings

Field	Description
Mobile Device	Select the check box to enable filtering on host data collected from mobile devices that are running the GlobalProtect app. Selecting this check box enables the Device , Settings , and Apps subtabs for editing.
Device subtab	<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.
Settings subtab	<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/jailbroken, select yes. To match devices that have not been rooted/jailbroken, select no. • Disk Encryption—Filter based on whether the device data has been encrypted. To match devices that have disk encryption enabled, select yes. To match devices that do not have disk encryption enabled, select no. • Time Since Last Check-in—Filter based on when the device last checked in with the MDM. Select an operator from the drop-down and then specify the number of days for the check-in window. For example, you could define the object to match devices that have not checked in within the last 5 days.
Apps subtab	<ul style="list-style-type: none"> • Apps—(Android devices only) Select this check box to enable filtering based on the apps that are installed on the device and whether or not the device has any malware-infected apps installed. • Criteria subtab <ul style="list-style-type: none"> – Has Malware—To match devices that have malware-infected apps installed select Yes; to match devices that do not have malware-infected apps installed, select No. If you do not want to use Has Malware as match criteria, select None. • Include subtab <ul style="list-style-type: none"> – Package—To match devices that have specific apps installed, click Add and then enter the unique app name (in reverse DNS format; for example, com.netflix.mediaclient) in the Package field and enter the corresponding app Hash, which the GlobalProtect app calculates and submits with the device HIP report.

Patch Management Tab

Use the **Patch Management** tab to enable HIP matching on the patch management status of the GlobalProtect clients.

Table 207. HIP Object Patch Management Settings

Field	Description
Patch Management	Select the check box to enable matching on the patch management status of the host. Selecting this check box enables the Criteria and Vendor subtabs for editing.
Criteria subtab	Specify the following settings on this subtab: <ul style="list-style-type: none"> • Is Enabled—Match on whether patch management software is enabled on the host. If the Is Installed check box is cleared, this field is automatically set to none and is disabled for editing. • Is Installed—Match on whether patch management software is installed on the host. • Severity—Match on whether the host has missing patches of the specified severity level. • Check—Match on whether the host has missing patches. • Patches—Match on whether the host has specific patches. Click Add and enter file names for the specific patch names to check for.
Vendor subtab	Use this subtab to define specific patch management software vendors and/or products to look for on the host to determine a match. Click Add and then choose a Vendor from the drop-down list. Optionally, click Add to choose a specific Product . Click OK to save the settings.

Firewall Tab

Use the **Firewall** tab to enable HIP matching based on the firewall software status of the GlobalProtect clients.

Table 208. HIP Object Firewall Settings

Field	Description
Firewall	Select the Firewall check box to enable matching on the firewall software status of the host: <ul style="list-style-type: none"> • Is Enabled—Match on whether firewall software is enabled on the host. If the Is Installed check box is cleared, this field is automatically set to none and is disabled for editing. • Is Installed—Match on whether firewall software is installed on the host. • Vendor and Product—Define specific firewall software vendors and/or products to look for on the host to determine a match. Click Add and then choose a Vendor from the drop-down list. Optionally, click Add to choose a specific Product. Click OK to save the settings. • Exclude Vendor—Select the check box to match hosts that do not have software from the specified vendor.

Antivirus Tab

Use the **Antivirus** tab to enable HIP matching based on the antivirus coverage on the GlobalProtect clients.

Table 209. HIP Object Antivirus Settings

Field	Description
Antivirus	<p>Select the check box to enable matching on the antivirus coverage on the host:</p> <ul style="list-style-type: none"> • Real Time Protection—Match on whether real-time antivirus protection is enabled on the host. If the Is Installed check box is cleared, this field is automatically set to none and is disabled for editing. • Is Installed—Match on whether antivirus software is installed on the host. • Virus Definition Version—Specify whether to match on whether the virus definitions have been updated within a specified number of days or release versions. • Product Version—Use this option to match against a specific version of the antivirus software. To specify a version to look for, select an operator from the drop-down and then enter a string representing the product version. • Last Scan Time—Specify whether to match based on the time that the last antivirus scan was run. Select an operator from the drop-down and then specify a number of Days or Hours to match against. • Vendor and Product—Define specific antivirus software vendors and / or products to look for on the host to determine a match. Click Add to and then choose a Vendor from the drop-down list. Optionally, click Add to choose a specific Product. Click OK to save the settings. • Exclude Vendor—Select the check box to match hosts that do not have software from the specified vendor.

Anti-Spyware Tab

Use the Anti-Spyware tab to enable HIP matching based on the anti-spyware coverage on the GlobalProtect clients.

Table 210. HIP Object Anti-Spyware Settings

Field	Description
Anti-Spyware	<p>Select the check box to enable matching on the anti-spyware coverage on the host and then define additional matching criteria for the match as follows:</p> <ul style="list-style-type: none"> • Real Time Protection—Match on whether real-time anti-spyware protection is enabled on the host. If the Is Installed check box is cleared, this field is automatically set to none and is disabled for editing. • Is Installed—Match on whether anti-spyware software is installed on the host. • Virus Definition Version—Specify whether to match on whether the virus definitions have been updated within a specified number of days or release versions. • Product Version—Use this option to match against a specific version of the anti-spyware software. To specify a version to look for, select an operator from the drop-down and then enter a string representing the product version. • Last Scan Time—Specify whether to match based on the time that the last anti-spyware scan was run. Select an operator from the drop-down and then specify a number of Days or Hours to match against. • Vendor and Product—Define specific anti-spyware software vendors and/or products to look for on the host to determine a match. Click Add to and then choose a Vendor from the drop-down list. Optionally, click Add to choose a specific Product. Click OK to save the settings. • Exclude Vendor—Select the check box to match hosts that do not have software from the specified vendor.

Disk Backup Tab

Use the Disk Backup tab to enable HIP matching based on the disk backup status of the GlobalProtect clients.

Table 211. HIP Object Disk Backup Settings

Field	Description
Disk Backup	Select the check box to enable matching on the disk backup status on the host and then define additional matching criteria for the match as follows: <ul style="list-style-type: none"> • Is Installed—Match on whether disk backup software is installed on the host. • Last Backup Time—Specify whether to match based on the time that the last disk backup was run. Select an operator from the drop-down and then specify a number of Days or Hours to match against. • Vendor and Product—Define specific disk backup software vendors and/or products to look for on the host to determine a match. Click Add to and then choose a Vendor from the drop-down list. Optionally, click Add to choose a specific Product. Click OK to save the settings. • Exclude Vendor—Select the check box to match hosts that do not have software from the specified vendor.

Disk Encryption Tab

Use the **Disk Encryption** tab to enable HIP matching based on the disk encryption status of the GlobalProtect clients.

Table 212. HIP Object Disk Encryption Settings

Field	Description
Disk Encryption	Select the check box to enable matching on the disk encryption status on the host:
Criteria	Specify the following settings on this subtab: <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: <ul style="list-style-type: none"> – Encrypted Locations—Enter specific locations to check for encryption on the host. – State—Specify how to match the state of the encrypted location by choosing an operator from the drop-down and then selecting a possible state (full, none, partial, not-available). Click OK to save the settings.
Vendor	Use this subtab to define specific disk encryption software vendors and/or products to look for on the host to determine a match. Click Add to and then choose a Vendor from the drop-down list. Optionally, click Add to choose a specific Product . Click OK to save the settings and return to the Disk Encryption tab.

Data Loss Prevention Tab

Use the **Data Loss Prevention** tab enable HIP matching based on whether or not the GlobalProtect clients are running data loss prevention software.

Table 213. HIP Object Data Loss Prevention Settings

Field	Description
Data Loss Prevention	<p>Select the check box to enable matching on the data loss prevention (DLP) status on the host (Windows hosts only) and then define additional matching criteria for the match as follows:</p> <ul style="list-style-type: none"> • Is Enabled—Match on whether DLP software is enabled on the host. If the Is Installed check box is cleared, this field is automatically set to none and is disabled for editing. • Is Installed—Match on whether DLP software is installed on the host. • Vendor and Product—Define specific DLP software vendors and/or products to look for on the host to determine a match. Click Add to and then choose a Vendor from the drop-down list. Optionally, click Add to choose a specific Product. Click OK to save the settings. • Exclude Vendor—Select the check box to match hosts that do not have software from the specified vendor.

Custom Checks Tab

Use the **Custom Checks** tab to enable HIP matching on any custom checks you have defined on the GlobalProtect portal. For details on adding the custom checks to the HIP collection, see “[Setting Up the GlobalProtect Portal](#)”.

Table 214. HIP Object Custom Checks Settings

Field	Description
Custom Checks	Select the check box to enable matching on any custom checks you have defined on the GlobalProtect portal.
Process List	To check the host system for a specific process, click Add and then enter the process name. By default, the agent checks for running processes; if you just want to check if a specific process is present on the system, clear the Running check box.
Registry Key	<p>To check Windows hosts for a specific registry key, click Add and enter the Registry Key to match on. To only match hosts that do not have the specified registry key, select the Key does not exist or match the specified value data check box.</p> <p>To match on specific values, click Add and then enter the Registry Value and Value Data. To match hosts that explicitly do not have the specified value or value data, select the Negate check box.</p> <p>Click OK to save the settings.</p>
Plist	<p>To check Mac hosts for a specific Property List (plist), click Add and enter the Plist name. To only match hosts that do not have the specified plist, select the Plist does not exist check box.</p> <p>To match on specific key-value pair within the plist, click Add and then enter the Key and the corresponding Value to match. To match hosts that explicitly do not have the specified key and/or value, select the Negate check box.</p> <p>Click OK to save the settings.</p>

Setting Up HIP Profiles

► *Objects > GlobalProtect > HIP Profiles*

Use this page to create the HIP profiles you will use to set up HIP-enabled security policies. A collection of HIP objects that are to be evaluated together, either for monitoring or for security policy enforcement. When you create your HIP profiles, you can combine the HIP objects you previously created (as well as other HIP profiles) using Boolean logic such that when a traffic flow is evaluated against the resulting HIP profile it will either match or not match. If there is a match, the corresponding policy rule will be enforced; if there is not a match, the flow will be evaluated against the next rule, as with any other policy matching criteria.

To create a HIP profile, click **Add**. The following table provides information on what to enter in the fields on the HIP Profile dialog. For more detailed information on setting up GlobalProtect and the workflow for creating HIP-augmented security policies, see “Configure HIP-Based Policy Enforcement” in the *GlobalProtect Administrator’s Guide*.

Table 215. HIP Profile Settings

Field	Description
Name	Enter a name for the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter an optional description.

Table 215. HIP Profile Settings (Continued)

Field	Description
Shared	<p>Select this check box if you want the HIP profile to be available to:</p> <ul style="list-style-type: none"> • All virtual systems (vsys) on the firewall, if you are logged in to a firewall that is in Multiple Virtual System Mode. If you clear the check box, the profile will be available only to the vsys selected in the Virtual System drop-down (Objects > GlobalProtect > HIP Profiles page). For a firewall that is not in Multiple Virtual System Mode, the check box does not appear in the HIP Profile dialog. • All device groups on Panorama. If you clear the check box, the profile will be available only to the device group selected in the Device Group drop-down (Objects > GlobalProtect > HIP Profiles page). <p>After you save the profile, you cannot change its Shared setting. The Objects > GlobalProtect > HIP Profiles page shows the current setting in the Location field.</p>
Match	<p>Click Add Match Criteria to open the HIP Objects/Profiles Builder.</p> <p>Select the first HIP object or profile you want to use as match criteria and then click add  to move it over to the Match text box on the HIP Profile dialog. Keep in mind that if you want the HIP profile to evaluate the object as a match only when the criteria in the object is not true for a flow, select the NOT check box before adding the object.</p> <p>Continue adding match criteria as appropriate for the profile you are building, making sure to select the appropriate Boolean operator radio button (AND or OR) between each addition (and, again, using the NOT check box when appropriate).</p> <p>If you are creating a complex Boolean expression, you must manually add the parenthesis in the proper places in the Match text box to ensure that the HIP profile is evaluated using the logic you intend. For example, the following expression indicates that the HIP profile will match traffic from a host that has either FileVault disk encryption (for Mac OS systems) or TrueCrypt disk encryption (for Windows systems) and also belongs to the required Domain, and has a Symantec antivirus client installed:</p> <pre>(("MacOS" and "FileVault") or ("Windows" and "TrueCrypt")) and "Domain" and "SymantecAV"</pre> <p>When you have finished adding the objects/profiles to the new HIP profile, click OK.</p>

Setting Up and Activating the GlobalProtect Agent

► *Device > GlobalProtect Client*

Use this page to download the GlobalProtect agent software to the firewall hosting the portal and activate it so that clients connecting to the portal can download it. You define how and when the software downloads occur—whether upgrades occur automatically when the agent connects, whether end users are prompted to upgrade, or whether upgrade is allowed at all for a particular set of users—in the client configurations you define on the portal. See the description of the [Agent Upgrade](#) field in the section that describes the portal ["Client Configuration Tab"](#) for more details. For details on the various options for distributing the GlobalProtect agent software and for step-by-step instructions for deploying the software, see “Deploy the GlobalProtect Client Software” in the [GlobalProtect Administrator’s Guide](#).



For initial download and installation of the GlobalProtect agent, the user on the client system must be logged in with administrator rights. For subsequent upgrades, administrator rights are not required.

The following table provides help for using this screen. For more detailed information on deploying agent software, see the [GlobalProtect Administrator's Guide](#).

Table 216. GlobalProtect Client Settings

Field	Description
Version	The version number of the GlobalProtect agent software that is available on the Palo Alto Networks Update Server. To check if a new agent software release is available from Palo Alto Networks, click Check Now . The firewall will use its service route to connect to the Update Server to check for new versions and, if there are updates available, display them at the top of the list.
Size	The size of the agent software bundle.
Release Date	The date and time Palo Alto Networks made the release available.
Downloaded	A check mark in this column indicates that the corresponding version of the agent software package has been downloaded to the firewall.
Currently Activated	A check mark in this column indicates that the corresponding version of the agent software has package has been activated on the firewall and can be downloaded by connecting agents. Only one version of the software can be activated at a time.
Action	Indicates the current action you can take for the corresponding agent software package as follows: <ul style="list-style-type: none"> • Download—The corresponding agent software version is available on the Palo Alto Networks Update Server. Click the link to initiate the download. If the firewall does not have access to the Internet, use an Internet-connected computer to go to the Software Update site to look for and Download new agent software versions to your local computer. Then click the Upload button on the GlobalProtect Client screen to manually upload the agent software to the firewall. • Activate—The corresponding agent software version has been downloaded to the firewall, but agents cannot yet download it. Click the link to activate the software and enable agent upgrade. To activate a software update that you manually uploaded to the firewall using the Upload button, you must click Activate From File button and select the version you want to activate from the drop-down (you may then need to refresh the screen for it to display as Currently Activated). • Reactivate—The corresponding agent software has been activated and is ready for client download. Because only one version of the GlobalProtect agent software can be active on the firewall at one time, if your end users require access to a different version than is currently active, you will have to Activate the other version to make it the Currently Active version.
Release Note	Provides a link to the GlobalProtect release notes for the corresponding agent version.
	Remove the previously downloaded agent software image from the firewall.

Setting Up the GlobalProtect Agent

The GlobalProtect agent (PanGP Agent) is an application that is installed on the client system (typically a laptop) to support GlobalProtect connections with portals and gateways and is supported by the GlobalProtect service (PanGP Service).



Make sure that you choose the correct installation option for your host operating system (32-bit or 64-bit). If installing on a 64-bit host, use 64-bit browser/Java combo for the initial installation.

To install the agent, open the installer file and follow the on-screen instructions.

To configure the agent:

1. Choose **Start > All Programs > Palo Alto Networks > GlobalProtect > GlobalProtect**.

The client interface opens to show the **Settings** tab.

2. Specify the username and password to use for GlobalProtect authentication, and optionally select the **Remember Me** check box.
3. Enter the IP address of the firewall that serves as the GlobalProtect Portal.
4. Click **Apply**.

Using the GlobalProtect Agent

The tabs in the GlobalProtect agent contain useful information about status and settings, and provide information to assist in troubleshooting connection issues.

- **Status tab**—Displays current connection status and lists any warnings or errors.
- **Details tab**—Displays information about the current connection, including portal IP addresses and protocol, and presents byte and packet statistics about the network connection.
- **Host State tab**—Displays the information stored in the HIP. Click a category on the left side of the window to display the configured information for that category on the right side of the window.
- **Troubleshooting tab**—Displays information to assist in troubleshooting.
 - **Network Configurations**—Displays the current client system configuration.
 - **Routing Table**—Displays information on how the GlobalProtect connection is currently routed.
 - **Sockets**—Displays socket information for the current active connections.
 - **Logs**—Allows you to display logs for the GlobalProtect agent (PanGP Agent) and service (PanGP Service). Choose the log type and debugging level. Click **Start** to begin logging and **Stop** to terminate logging.

Chapter 10

Configuring Quality of Service

This section describes how to configure quality of service (QoS) on the firewall:

- [“Configuring QoS for Firewall Interfaces”](#)
- [“Defining QoS Profiles”](#)
- [“Defining QoS Policies”](#)
- [“Displaying QoS Statistics”](#)

Configuring QoS for Firewall Interfaces

► *Network > QoS*

Use the **QoS** page to configure bandwidth limits for firewall interfaces.

Table 217. QoS Settings

Field	Description
Physical Interface	
Interface Name	Select the firewall interface.
Egress Max (Mbps)	Enter the limit on traffic leaving the firewall through this interface. <i>Note:</i> Though this is not a required field, it is recommended to always define the Egress Max value for a QoS interface.
Turn on QoS feature on this interface	Select the check box to enable QoS features.
Default Profile: Clear Text Tunnel Interface	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, see “Defining QoS Profiles” .
Clear Text Traffic and Tunneled Traffic	Specify the following settings on the Clear Text Traffic tab and the Tunneled Traffic tabs.

Table 217. QoS Settings (Continued)

Field	Description
Egress Guaranteed (Mbps)	Enter the bandwidth that is guaranteed for clear traffic from this interface.
Egress Max (Mbps)	Enter the limit on 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, see “Defining QoS Profiles”. – 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, select the check box for 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>

Defining QoS Profiles

► *Network > Network Profiles > QoS Profiles*

For each interface, you can define QoS profiles that determine how the QoS traffic classes are treated. You can set overall limits on bandwidth regardless of class and also set limits for individual classes. You can also assign priorities to different classes. Priorities determine how traffic is treated in the presence of contention.

Click **Add** and complete the fields described in to define a QoS profile.



See “Configuring QoS for Firewall Interfaces” for information on configuring firewall interfaces for QoS and see “Defining QoS Policies” to configure the policies that will activate the QoS restrictions.

Table 218. QoS Profile Settings

Field	Description
Profile Name	Enter a name to identify the profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Egress Max	Enter the maximum bandwidth allowed for this profile (Mbps). The Egress Max value for a QoS profile must be less than or equal to the Egress Max value defined for the physical interface that QoS is enabled on. See “Configuring QoS for Firewall Interfaces”. <i>Note:</i> Though this is not a required field, it is recommended to always define the Egress Max value for a QoS profile.
Egress Guaranteed	Enter the bandwidth that is guaranteed for this profile (Mbps).
Classes	Click Add to specify how to treat individual QoS classes. You can select one or more classes to configure: <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 • 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. <i>Note:</i> Though this is not a required field, it is recommended to always define the Egress Max value for a QoS profile. Egress Guaranteed —Click and enter the guaranteed bandwidth (Mbps) for this class. When contention occurs, traffic that is assigned a lower priority is dropped. Real-time priority uses its own separate queue.

Defining QoS Policies

► Policies > QoS

The QoS policy determines how traffic is classified for treatment when it passes through an interface with QoS enabled. For each rule, specify one of eight classes. You can also assign a schedule to specify which rule is active. Unclassified traffic is automatically assigned to class 4.

For information on defining policies on Panorama, see [“Defining Policies on Panorama”](#).

Click **Add** to open the **QoS Policy Rule** dialog. The **QoS Policy Rule** dialog contains six subtabs, described in Table 219:

- “General Tab”
- “Source Tab”
- “Description”
- “Application Tab”
- “Service/ URL Category Tab”



See [“Configuring QoS for Firewall Interfaces”](#) for information on configuring firewall interfaces for QoS and see [“Defining QoS Profiles”](#) for information on configuring classes of service.

Use the QoS Policy page to perform several actions, including:

- To view just the rules for a specific virtual system, select the system from the **Virtual System** drop-down list and click **Go**.
- To apply a filter to the list, select from the **Filter Rules** drop-down list.
- To view just the rules for specific zones, select a zone from the **Source Zone** and/or **Destination Zone** drop-down lists, and click **Filter by Zone**.



Shared policies pushed from Panorama are shown in green and cannot be edited at the device level.

- To add a new QoS rule, do one of the following:
 - Click **Add** at the bottom of the page and configure the rule. A new rule is added to the bottom of the list.
 - Select **Clone Rule**, or select a rule by clicking the white space of the rule, and select **Clone** at the bottom of the page (a selected rule has a blue background). The copied rule is inserted below the selected rule.

Table 219. QoS Rule Settings

Field	Description
General Tab	
Name	Enter a name to identify the rule (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter an optional description.
Tag	If you need to tag the policy, click Add to specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword. For example, you may want to tag certain security policies with Inbound to DMZ, decryption policies with the words Decrypt and No-decrypt, or use the name of a specific data center for policies associated with that location.
Source Tab	
Source Zone	Select one or more source zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire).
Source Address	<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 list and do any of the following:</p> <ul style="list-style-type: none"> Select the check box next to the appropriate addresses  and/or address groups  in the Available column, and click Add to add your selections to the Selected column. Enter the first few characters of a name in the Search field to list all addresses and address groups that start with those characters. Selecting an item in the list will set the check box in the Available column. Repeat this process as often as needed, and then click Add. Enter one or more IP addresses (one per line), with or without a network mask. The general format is: <code><ip_address>/<mask></code> To remove addresses, select the appropriate check boxes in the Selected column and click Delete, or select any to clear all addresses and address groups. <p>To add new addresses that can be used in this or other policies, click New Address. To define new address groups, see “Defining Address Groups” .</p>
Source User	Specify the source users and groups to which the QoS policy will apply.
Negate	Select the check box to have the policy apply if the specified information on this tab does NOT match.
Destination Zone	Select one or more destination zones (default is any). Zones must be of the same type (Layer 2, Layer 3, or virtual wire).

Table 219. QoS Rule Settings (Continued)

Field	Description
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 list and do any of the following:</p> <ul style="list-style-type: none"> Select the check box next to the appropriate addresses  and/or address groups  in the Available column, and click Add to add your selections to the Selected column. Enter the first few characters of a name in the Search field to list all addresses and address groups that start with those characters. Selecting an item in the list will set the check box in the Available column. Repeat this process as often as needed, and then click Add. Enter one or more IP addresses (one per line), with or without a network mask. The general format is: <code><ip_address>/<mask></code> To remove addresses, select the appropriate check boxes in the Selected column and click Delete, or select any to clear all addresses and address groups. <p>To add new addresses that can be used in this or other policies, click New Address (see “Defining Applications”). To define new address groups, see “Defining Address Groups”.</p>
Negate	Select the check box to have the policy apply if the specified information on this tab does NOT match.
Application Tab	
Application	<p>Select specific applications for the QoS rule. To define new applications, see “Defining Applications”. To define application groups, see “Defining Application Groups”.</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 list:</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. See “Services” and “Service Groups”.

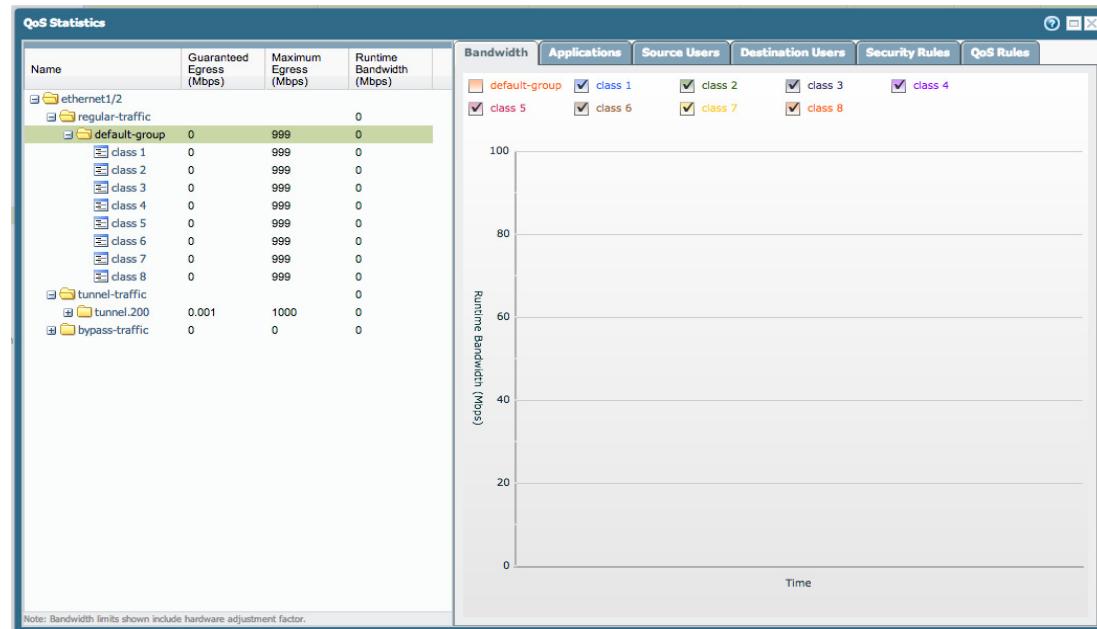
Table 219. QoS Rule Settings (Continued)

Field	Description
URL Category	Select URL categories for the QoS rule. <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 list. You can add multiple categories. See “Dynamic Block Lists” for information on defining custom categories.
Class	Choose the QoS class to assign to the rule, and click OK . Class characteristics are defined in the QoS profile. See “Defining QoS Profiles” for information on configuring settings for QoS classes.
Schedule	Choose the calendar icon to set a schedule for the QoS policy to apply.

Displaying QoS Statistics

► *Network > QoS*

The table on the **QoS Policies** page indicates when QoS is enabled, and includes a link to display QoS statistics. An example is shown in the following figure.

Figure 15. QoS Statistics

The left panel shows the QoS tree table, and the right panel shows data in the following tabs:

- **QoS Bandwidth**—Shows the real time bandwidth charts for the selected node and classes. The information is updated every two seconds.

NOTE: The QoS Egress Max and Egress Guaranteed limitations configured for the QoS classes might be shown with a slightly different value in the QoS Statistics screen. This is normal behavior and is caused by how the hardware engine summarizes bandwidth limits and counters. There is no operational concern as the bandwidth utilization graphs display the real-time values and quantities.

- **Session Browser**—Lists the active sessions of the selected node and/or class.
- **Application View**—Lists all active applications for the selected QoS node and/or class.

Chapter 11

Central Device Management Using Panorama

Panorama, available both as a dedicated hardware platform and as a VMware virtual appliance, is the centralized management system for the Palo Alto Networks family of next-generation firewalls. It shares the same web-based look and feel as the individual firewall interface, and allows you to seamlessly transition in to managing the firewalls centrally and reducing the administrative effort in managing multiple firewalls.

This section serves as a field reference for using the Panorama web interface to manage the firewalls on your network. For information on setting up Panorama, Panorama concepts and workflows, see the *Panorama Administrator's Guide*.

- [“Panorama Tab”](#)
- [“Switching Device Context”](#)
- [“Setting Up Storage Partitions”](#)
- [“Configuring High Availability \(HA\)”](#)
- [“Adding Devices”](#)
- [“Backing Up Firewall Configurations”](#)
- [“Defining Device Groups”](#)
- [“Defining Panorama Administrator Roles”](#)
- [“Creating Panorama Administrative Accounts”](#)
- [“Specifying Panorama Access Domains for Administrators”](#)
- [“Logging and Reporting”](#)
- [“Managing Log Collectors”](#)
- [“Defining Log Collector Groups”](#)
- [“Generating User Activity Reports”](#)
- [“Viewing Firewall Deployment Information”](#)

- “Scheduling Dynamic Updates”
- “Scheduling Configuration Exports”
- “Upgrading the Panorama Software”
- “Register VM-Series Firewall as a Service on the NSX Manager”

Panorama Tab

► Panorama

The **Panorama** tab is similar to the **Devices** tab for the firewall, but the settings apply to the Panorama server, not the managed firewalls. The following table describes the pages on this tab. To access a page, click the page name link on the side menu.

Table 220. Summary of Panorama Pages

Page	Description
Setup	Allows you to specify the Panorama host name, the network settings of the management interface, and the addresses of network servers (DNS and NTP). See “ Defining Management Settings ”.
Templates	Allows you to create Templates that can be used to manage configuration options based on the Device and Network tabs. Templates enable you to reduce administrative effort in deploying multiple firewalls with similar configuration. See “ Templates ”.
Config Audit	Allows you to view and compare configuration files. See “ Defining Operations Settings ” and “ Switching Device Context ”.
Managed Devices	Allows you to add firewalls for management by Panorama, push shared configuration to managed firewalls, and run comprehensive configuration audits on firewalls or entire device groups. See “ Adding Devices ”.
Device Groups	Allows you to group firewalls based on function, network segmentation, or geographic location. A device group can include physical firewalls, virtual firewalls and/or a virtual system. 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. See “ Defining Device Groups ”.
Managed Collectors	Allows you to configure and manage the log collector devices (the M-100 appliance configured to function in <i>Log Collector</i> mode or as a dedicated Log Collector). Because a dedicated Log Collector is configured and managed using Panorama, it is also called a Managed Collector. A Managed Collector be managed by either an M-100 appliance in Panorama mode or by a Panorama virtual appliance. The v5.0 and later firewalls managed by Panorama can send logs to these managed collectors. You can also use this tab to upgrade the software on your log collectors. You first download the latest Panorama software and you can then push the updated version to your log collectors by clicking Install on the Managed Collectors page. <i>Note:</i> The M-100 appliance can be configured as a Panorama manager, a log collector, or both. The operational command to change the mode of an M-100 is request system logger-mode [panorama logger] . To view the current mode, run show system info match logger_mode . When an M-100 appliance is in log collector mode, only the CLI is available for management. See “ Managing Log Collectors ”.

Table 220. Summary of Panorama Pages (Continued)

Page	Description
Collector Groups	<p>Allows you to logically group one or more log collectors so you can apply the same configuration settings to all log collectors in a <i>collector group</i>, and then assign firewalls to the log collectors. The logs are uniformly distributed amongst all the disks in a Log Collector and across all members in the Collector Group.</p> <p>Each Panorama can have up to 16 collector groups, and each collector group can have up to 16 log collectors. For configuring a log collector group, see “Adding a Log Collector”.</p>
Admin Roles	Allows you to specify the privileges and responsibilities that are assigned to users who require access to Panorama. See “Defining Administrator Roles” .
Password Profiles	<p>Allows you to define password profiles, which can then be applied to Panorama administrators. You can configure the following profile options:</p> <ul style="list-style-type: none"> • Required password change period (days) • Expiration warning period (days) • Post Expiration Admin Login Count • Post Expiration Grace Period (days)
Administrators	<p>Allows you to define the accounts for users who require access to Panorama. See “Creating Administrative Accounts”.</p> <p>Note: A lock icon displays in the right column on the Administrators page, if a user account is locked out. The administrator can click the icon to unlock the account.</p>
High Availability	Allows you to configure a pair of Panorama devices to support high availability (HA). See “Configuring High Availability (HA)” .
Certificate Management	Allows you to configure and manage certificates, certificate profiles, and keys. See “Managing Device Certificates” .
Log Settings	Allows you to define Simple Network Management Protocol (SNMP) trap sinks, syslog servers, and email addresses for distributing log messages.
Server Profiles	<p>Allows you to specify profiles for servers that provide services to Panorama. See the following sections:</p> <ul style="list-style-type: none"> • “Configuring Email Notification Settings” • “Configuring SNMP Trap Destinations” • “Configuring Syslog Servers” • “Configuring RADIUS Server Settings” • “Configuring LDAP Server Settings” • “Configuring Kerberos Settings (Native Active Directory Authentication)” • “Configuring Netflow Settings”
Authentication Profile	Allows you to specify a profile to authentication access to Panorama. See “Setting Up Authentication Profiles” .
Authentication Sequence	Allows you to specify the chain of authentication realms to use for permitting access to Panorama. See “Setting Up an Authentication Sequence” .
Access Domain	When used with RADIUS authentication, Access Domains allow you to use Vendor Specific Attributes (VSA) to limit administrative access to Device Groups, Templates, and the Device Contexts that administrators can manage. See “Specifying Panorama Access Domains for Administrators” .

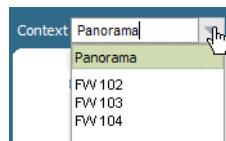
Table 220. Summary of Panorama Pages (Continued)

Page	Description
Scheduled Config Export	Allows you to collect running configurations from Panorama and managed firewalls and deliver them daily to a File Transfer Protocol (FTP) server or by using Secure Copy (SCP) to securely transfer data between the Panorama server and a remote host. See “ Scheduling Configuration Exports ”.
Software	Allows you to view the available Panorama software releases and download and install a selected software version. See “ Upgrading the Panorama Software ”.
Dynamic Updates	Allows you to view the latest application definitions and information on new security threats, such as antivirus signatures (threat prevention license required) and update Panorama with the new definitions. See “ Updating Threat and Application Definitions ”.
Support	Allows you to access product and security alerts from Palo Alto Networks. See “ Viewing Support Information ”.
Device Deployment	Allows you to view current license information on the managed firewalls and install software, clients, and dynamic content on the managed firewalls and managed collectors. See “ Viewing Firewall Deployment Information ”. To automate the process of downloading and installing dynamic updates, see “ Scheduling Dynamic Updates ”.
Master Key and Diagnostics	Allows you to specify a master key to encrypt private keys on the firewall. Private keys are stored in encrypted form by default even if a new master key is not specified. See “ Encrypting Private Keys and Passwords on the Firewall ”.

Switching Device Context

Switching context allows an administrator to launch the web interface of a managed firewall from the Panorama web interface. It allows you to use Panorama to directly access and manage firewall-specific settings on an individual firewall (such as firewall-specific policy, networking, and device setup).

Use the **Context** drop-down list above the side menu to choose an individual firewall or the full Panorama view. The context menu displays the firewalls to which you have administrative access (see “Panorama Administrator Roles, Profiles, and Accounts” on page 386). Use the filters to refine your search criteria; when you select a firewall, the web interface refreshes to show all the device tabs and options for the selected firewall.

**Figure 16. Choosing Context**

You can only switch context to connected firewalls. Disconnected firewalls are not shown in the drop-down list.

Setting Up Storage Partitions

► *Panorama > Setup > Operations > Storage Partition Setup*

By default, the Panorama virtual appliance has a single disk partition for all data in which, regardless of the total disk size, 10.89GB is allocated for log storage. Increasing the disk size doesn't increase the log storage capacity. To modify the log storage capacity, your options are:

- [Add another virtual disk](#) of up to 2TB.
- Mount Panorama to a Network File System (NFS)—Click **Storage Partition Setup** in the Miscellaneous section, set the **Storage Partition** to **NFS V3**, and complete the fields in Table 221.
- Revert to the default internal storage partition if you previously configured another virtual disk or mounted to an NFS—Click **Storage Partition Setup** in the Miscellaneous section and set the **Storage Partition** to **Internal**.



You must reboot the Panorama management server after configuring the storage partition settings. Select Panorama > Setup > Operations and click Reboot Panorama.

Table 221. Panorama Storage Partition Setup—NFS V3

Field	Description
Server	Specify the FQDN or IP address of the NFS server.
Log Directory	Specify the full path name of the directory where the logs will reside.
Protocol	Specify the protocol (UDP or TCP) for communication with the NFS server.
Port	Specify the port for communication with the NFS server.
Read Size	Specify the maximum size in bytes (range is 256-32768) for NFS read operations.
Write Size	Specify the maximum size in bytes (range is 256-32768) for NFS write operations.
Copy on Setup	Select the check box to mount the NFS partition and copy any existing logs to the destination directory on the server when Panorama boots.
Test Logging Partitions	Click to perform a test that mounts the NFS partition and presents a success or failure message.

Configuring High Availability (HA)

► *Panorama > High Availability*

High availability (HA) allows for redundancy in the event of a failure. For ensuring HA, you can deploy a pair of hardware-based Panorama appliances or a pair of Panorama virtual appliances in a HA peer configuration that provide synchronized connections to the managed firewalls. Among the peers in the HA configuration, one device must be designated as primary and the other as secondary; the primary device will assume the active state and the secondary device will take the passive state, until a monitored metric fails. The peers maintain a heartbeat, or a periodic ICMP ping, to verify operational status. If the active Panorama server becomes unavailable, the passive server takes over temporarily. With preemption enabled, the default setting, when the active Panorama server becomes available again, the passive server relinquishes control and returns to the passive state.



To configure a HA pair of Panorama virtual appliances, you must have two Panorama licenses with unique serial numbers for each virtual instance.

To enable HA on Panorama, configure the followings settings:

Table 222. Panorama HA Settings

Field	Description
Setup	
Enable HA	Select the check box to enable HA.
Peer HA IP Address	Enter the IP address of the MGT interface of the peer.
Enable Encryption	<p>Enable encryption after exporting the HA key from the HA peer and importing it onto this device. The HA key on this device must also be exported from this device and imported on the HA peer. When enabled, the MGT interface encrypts communication between the HA peers.</p> <p>The key import/export is done on the Certificates page. See “Managing Device Certificates”.</p> <p><i>Note: HA connectivity uses TCP port 28 with encryption enabled and 28769 when encryption is not enabled.</i></p>
Monitor Hold Time (ms)	Enter the length of time (ms) that the system will wait before acting on a control link failure (1000-60000 ms, default 3000 ms).
Election Settings	
Priority (Only required on virtual Panorama)	<p>Assign a device as Primary and the other as Secondary in each pair.</p> <p>This primary or secondary configuration determines which peer is designated as the primary recipient for logs sent by the managed firewalls. You can configure Panorama to use the same log external storage facility for the assigned primary and secondary devices (Network File System or NFS option) or configure logging internally. If you use the NFS option, only the primary recipient receives the logs that are sent from the managed firewalls. However, if local logging is enabled, by default the logs are sent to both the primary and the secondary recipient.</p>
Preemptive	Select the check box to enable the primary Panorama device to resume active operation after recovering from a failure. If this setting is off, then the secondary device remains active even after the higher priority device recovers from a failure.
Preemption Hold Time (min)	Enter the time a passive device will wait before taking over as the active device (range 1-60 min, default 1).
Promotion Hold Time (ms)	Enter the time that the secondary device will wait before taking over (range 0-60000 ms, default 2000).
Hello Interval (ms)	Enter the number of milliseconds between the hello packets sent to verify that the other device is operational (ranges 8000-60000 ms, default 8000).
Heartbeat Interval (ms)	Specify how frequently Panorama sends ICMP pings to the HA peer (range 1000-60000 ms, default 1000).
Monitor Fail Hold Up Time (ms)	Specify the interval that Panorama waits following a path monitor failure before attempting to re-enter the passive state (default 0 ms). During this period, the device is not available to take over for the active device in the event of failure.

Table 222. Panorama HA Settings (Continued)

Field	Description
Additional Master Hold Up Time (ms)	Specify the interval during which the preempting device remains in the passive state before taking over as the active device (default 7000 ms).
Path Monitoring	
Enabled	Select the check box to enable path monitoring. Path monitoring enables Panorama to monitor specified destination IP addresses by sending ICMP ping messages to make sure that they are responsive.
Failure Condition	Select whether a failover occurs when any or all of the monitored path groups fail to respond.
Path Groups	Define one or more path groups to monitor specific destination addresses. To add a path group, specify the following and click Add : <ul style="list-style-type: none"> • Name—Specify a name for the path group. • Enabled—Select the check box to enable the path group. • Failure Condition—Select whether a failure occurs when any or all of the specified destination addresses fails to respond. • Destination IPs—Enter one or more destination addresses to be monitored (multiple addresses must be separated by commas). • Ping Interval—Specify the interval between pings that are sent to the destination address (range 1000-60000 milliseconds, default 5000 milliseconds). • Ping Count—Specify the number of failed pings before declaring a failure (range 3-10 pings, default 3 pings). To delete a path group, select the group, and click Delete .

Adding Devices

► *Panorama > Managed Devices*

A Palo Alto Networks firewall that Panorama manages is called a managed device. The **Managed Devices** page allows you to perform tasks such as adding firewalls for centralized management, perform software upgrades, and manage configuration backups. It also displays information on the status of each managed device.

To enable the firewalls to connect to the Panorama server and be centrally managed, you must complete the following two-steps:

- Add the firewall serial number on the Panorama server.
- Add the IP address of the Panorama server on the firewall.



Panorama can manage PAN-OS firewalls running the same major release or earlier supported versions, but not firewalls running a later release version. For example, Panorama 5.0 can manage PAN-OS firewalls running 5.0 or earlier supported versions, but it cannot manage PAN-OS firewalls running 5.1.

The **Managed Devices** page allows you to perform the following tasks:

- **Add Devices:** To add a firewall, click **Add** and enter the serial number of one or more firewalls. Make sure to enter only one entry per row.

- **Install:** To perform a software or content update, click **Install** and fill in the following details: .

Table 223. Software/Content Update on a Managed Device

Field	Description
Type	Select the type of update you want to install.
File	Select a file from the list of Uploaded or Downloaded files. You must have either downloaded an image using the Panorama > Device Deployment subtabs or have used the Install from file option to upload a file to Panorama.
Devices	Use the filters to select the firewalls on which you want to install the image.
Upload only to device (do not install)	Select this option if you would like to upload the image on the firewall, but do not want to reboot the firewall now. Until you initiate a reboot, the latest software image will not be installed.
Reboot device after install	Select this option if you want to upload and install the latest software image. A reboot will be triggered.

Group HA Peers: For firewalls that are deployed in an HA configuration, select the HA peers and select the **Group HA Peers** check box to group firewalls in HA mode together.

This option allows you to easily identify firewalls that are in HA mode. When pushing shared policies, you can push to the grouped pair, instead of each firewall individually. Also, when adding a new firewall in Managed Devices, if they are in HA mode, both firewalls will be displayed together, so you can add both firewalls.

When viewing an HA pair, if the configuration does not match, a warning indicator will appear. You will also see an indicator if the HA firewalls are in different device groups. When viewing an HA pair, if the configuration does not match a warning indicator will appear. You will also see an indicator if the HA firewalls are in different device groups. For HA peers in a active-passive configuration, consider adding both firewalls or virtual systems of the peers (if in multi-virtual system mode) to the same device group. This allows you to push the configuration to both HA peer firewalls at the same time.

This option is also independent for each section, so enabling and disabling in one area, will not enable/disable for all areas. The **Group HA Peers** option is present in the following Panorama areas:

- Managed Devices
- Templates
- Device Groups
- **Policies tab (Target tab for all policy types)**
- Commit dialog

Delete: Select the check box for one or more firewalls and click **Delete** to remove the firewall from the list of firewalls that Panorama manages.

Tag: Select the check box for one or more firewalls and click **Tag** to add tags. Enter a text string of up to 31 characters. Do not use an empty space.

Tags make it easier for you to find a firewall from a large list; they help you to dynamically filter and refine the list of firewalls that display. For example, if you add a tag called branch office, you can filter for all branch office firewalls across your network.

The **Managed Devices** page lists each managed firewall along with the information listed in the following table.

Table 224. Status of the Managed Devices

Field	Description
Device Name	Displays the hostname or the serial number of the firewall you have added.
Virtual System	Lists the virtual systems available on a firewall enabled for multi virtual system capability.
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 to which the firewall belongs.
Status	Connected—Displays whether Panorama is connected or disconnected with the firewall. Shared Policy—Displays whether the configuration (Policies and Objects) is in sync or out of sync with Panorama. Template—Displays whether the configuration (network and device) is synchronized with Panorama. Last Commit State—Displays whether the last commit failed or succeeded on the firewall. Software, Apps and Threat, Antivirus, URL Filtering GlobalProtect Client and WildFire—Displays the version of software/content that is currently installed on the managed firewall.
Backups	On each commit, a configuration backup of the managed firewall is automatically sent to Panorama. The Manage... link allows you to view the configuration backups available. To load a version from the list of saved configuration files, click Load .

Backing Up Firewall Configurations

► *Panorama > Managed Devices*

Panorama automatically saves every configuration change you commit to the managed firewalls. To configure the number of versions to keep on the Panorama device, select **Panorama > Setup > Management**, edit the Logging and Reporting Settings, select the **Log Export and Reporting** tab, and enter a value (default 100) in the **Number of Versions for Config Backups** field.

To manage backups on Panorama, select **Panorama > Managed Devices** and, in the **Backups** column for a device, click **Manage**. A window opens to show the saved and committed configurations for the device. Click a **Load** link to restore the backup to the candidate configuration, and then make any desired changes and click **Commit** to restore the loaded configuration to the device. To remove a saved configuration, click the  icon.

Defining Device Groups

► *Panorama > Device Groups*

Device groups in Panorama allow you to group firewalls and then define policies and objects that can be shared all device groups or shared amongst the firewalls in a device group. Because device groups are designed to help scale and manage shared policies and objects, before you create device groups you must plan on how you would like to group your firewalls. For example, you could create device groups based on similar functionality, security requirements, or geographic location.

Device groups can consist of firewalls and/or virtual systems that you want to manage as a group, such as the firewalls that manage a group of branch offices or individual departments in a company. Each group is treated as a single unit when applying policies in Panorama.

A firewall can belong to only one device group. Because virtual systems are considered distinct entities in Panorama, you can assign virtual systems within a firewall to different device groups.

The Device Groups page allows you to add, delete, and view the device groups configured on Panorama.

To add a device group, click **Add** and provide the information listed in the following table.

Table 225. Device Group Settings

Field	Description
Device Group 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.
Description	Enter a description for the group.
Devices	Select the check box for each firewall that you want to add to the device group. Click OK to save the changes to the device group. Use the filters to refine the list of firewalls that display. By default, the filter displays the entire list of managed firewalls grouped by Templates, Platforms, Tags ; it also displays the numerical value of the total number of managed firewalls and when you select the check box for your filtering criteria, it displays the number of firewalls in your selected criteria as a fraction of the total number of managed firewalls.

Table 225. Device Group Settings (Continued)

Field	Description
Master Device	Select a device to use as the master. The master device is the firewall from which Panorama gathers User-ID information for use in policies. The gathered user and group mapping information is specific to a device group and can come from only one device (the master) inside the group.
Group HA Peers	Select the check box to group firewalls in high availability (HA) mode together. This option allows you to easily identify firewalls that are in HA mode. When pushing shared policies, you can push to the grouped pair, instead of each firewall individually. Also, when adding a new firewall in Managed Devices, if they are in HA mode, both firewalls will be displayed together, so you can add both firewalls. When viewing an HA pair, if the configuration does not match a warning indicator will appear. You will also see an indicator if the HA firewalls are in different device groups. For HA peers in a active-passive configuration, consider adding both firewalls or virtual systems of the peers (if in multi-virtual system mode) to the same device group. This allows you to push the configuration to both HA peer firewalls at the same time.

After creating a device group, you must commit your changes to Panorama and to the device group; when you commit your changes, the configuration changes are pushed to the managed firewalls that are assigned to the device group. For information on committing your changes to Panorama, see [“Committing your Changes in Panorama”](#)

Delete: Select the check box for one or more device groups and click **Delete** to remove the device group.

Shared Objects and Policies

Device Groups provide a way to implement a layered approach for managing policies across the network of managed firewalls. A shared object or rule can be used across any/all device groups. A device group specific object can only be used by the device group that it belongs to. Only Panorama administrators can create shared policies and objects.

- To create a shared policy, on the **Policies** tab, select **Shared** from the **Device Groups** drop-down list.



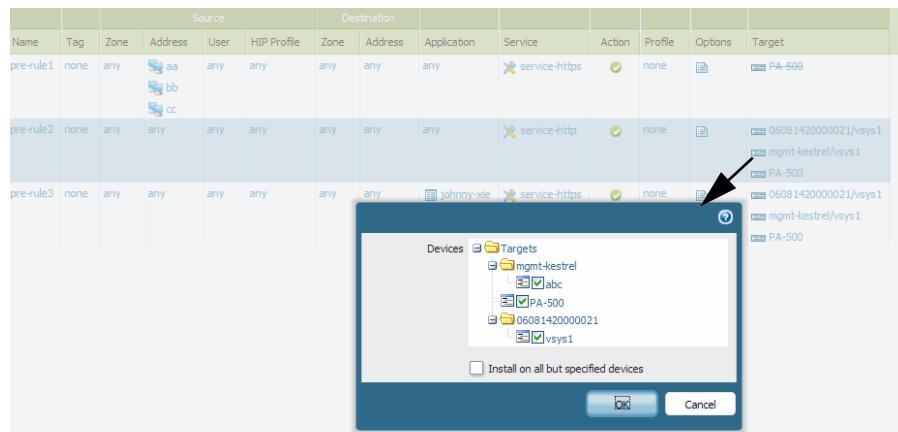
- To create device group specific policy, on the **Policies** tab, select the appropriate device group from the **Device Groups** drop-down list.
- To create a shared object, on the **Objects** tab, click **Add** and select the **Shared** check box when defining the object.

- To create device group specific objects, on the **Objects** tab, select the appropriate device group from the **Device Groups** drop-down list.

Note: If you have objects of the same name where one is shared and another is device group specific, the device group specific object will be used for that device group.

Applying Policy to a Specific Device in a Device Group

You can target a policy rule to individual firewalls within the device group for which the rule is defined. To target a firewall after a policy is created, click an entry in the **Target** column and select the firewalls in the pop-up window. To apply the rule to all firewalls in a device group EXCEPT the targeted firewall, select the **Install on all but specified devices** check box.



Name	Tag	Zone	Source			Destination			Application	Service	Action	Profile	Options	Target
			Address	User	HIP Profile	Zone	Address							
pre-rule1	none	any	aa bb cc	any	any	any	any	any	service-https	green checkmark	none	edit icon		PA-500
pre-rule2	none	any	any	any	any	any	any	any	service-http	green checkmark	none	edit icon		06081420000021/vsys1 mgmt-kestrel/vsys1 PA-500
pre-rule3	none	any	any	any	any	any	any	johnny-xie	service-https	green checkmark	none	edit icon		06081420000021/vsys1 mgmt-kestrel/vsys1 PA-500

Figure 17. Targeting Policy Rules to Individual Devices in Panorama

Defining Panorama Administrator Roles

► *Panorama > Admin Roles*

Use the **Admin Roles** page to define role profiles that determine the access and responsibilities available to administrative users. For instructions on adding administrator accounts, see “[Creating Panorama Administrative Accounts](#)”.

Panorama administrators who do not have access to the **Panorama > Administrators** page, can click on their username located to the left of the logout link on the bottom of the web interface to change their password.



The Admin Role can be mapped via RADIUS Vendor-Specific Attributes (VSA) using the following attribute: “PaloAlto-Panorama-Admin-Role = <AdminRoleName>,”.

Table 226. Panorama Administrator Role Settings

Field	Description
Name	Enter a name to identify this administrator role (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter an optional description of the role.
Permission	Select the scope of administrative responsibility (Panorama or Device Group and Template).
WebUI	Click the icons for specified areas to indicate the type of access permitted for the web interface: <ul style="list-style-type: none"> • Read/write access to the indicated page. • Read only access to the indicated page. • No access to the indicated page.
XML API	Select the type of access for the XML API <ul style="list-style-type: none"> • Report—Access to the firewall reports. • Log—Access to the firewall logs. • Configuration—Permissions to retrieve or modify the firewall configuration. • Operational Requests—Permissions to run operational commands. • Commit—Permissions to commit the configuration. • User-ID Agent—Access to the User-ID Agent. • Export—Permissions to export files from the firewall, including the configuration, block or response pages, certificates, keys, and more. • Import—Permissions to import files to the firewall, including software, content, license, configuration, certificates, block pages, custom logs, and more.
Command Line	Select the type of role for CLI access: <ul style="list-style-type: none"> • None—Access to the firewall CLI not permitted. • superuser—Full access to the current firewall. • superreader—Read-only access to the current firewall. • panorama-admin—Full access to a selected firewall, except for defining new accounts or virtual systems.

Creating Panorama Administrative Accounts

► *Panorama > Administrators*

Administrator accounts control access to Panorama. Each administrator can have full or read-only access to Panorama and all managed firewalls, or can have Panorama administrator access, which allows access to the Panorama configuration (except administrator accounts and roles) but not the managed firewalls. The predefined **admin** account has full access to Panorama and the managed firewalls.

Panorama supports the following authentication options:

- Password authentication—The administrator enters a username and password to log in. This authentication requires no certificates. You can use it in conjunction with authentication profiles, or for local database authentication.
- Client certificate authentication (web)—This authentication requires no username or password; the certificate suffices to authenticate access to Panorama.
- Public key authentication (SSH)—The administrator generates a public/private key pair on the machine that requires access to Panorama, and then uploads the public key to Panorama to allow secure access without requiring the administrator to enter a username and password.

Table 227. Administrator Account Settings

Field	Description
Name	Enter a login name 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 for administrator authentication. You can use this setting for RADIUS, LDAP, Kerberos, or local database authentication. For more details, see “Setting Up Authentication Profiles” .
Use only client certificate authentication (Web)	Select the check box to use client certificate authentication for web access. If you select this check box, a username and password are not required; the certificate is sufficient to authenticate access to 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 mixture of lower-case letters, upper-case letters, and numbers. You can also enforce Minimum Password Complexity from the Panorama > Setup > Management tab. Certain Panorama administrators might not have access to the Panorama > Administrators page. In this case, to change his or her local password, the administrator can click his or her username located to the left of the logout link on the bottom of the web interface.

Table 227. Administrator Account Settings (Continued)

Field	Description
Use Public Key Authentication (SSH)	Select the check box to use SSH public key authentication. Click Import Key and browse to select the public key file. The uploaded key is displayed in the read-only text area. Supported key file formats are IETF SECSH and OpenSSH. Supported key algorithms are DSA (1024 bits) and RSA (768-4096 bits). Note: If the public key authentication fails, a login and password prompt is presented to the administrator.
Role	Assign a role to this administrator. The role determines what the administrator can view and modify. <ul style="list-style-type: none">• Dynamic—You can select any of the following pre-configured roles from the drop-down:<ul style="list-style-type: none">– Superuser—Full 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 administrator accounts and roles) and all device groups and templates. No access to managed firewalls.• Role Based—Access based on the custom role (see “Defining Panorama Administrator Roles”) you select in the drop-down. If you select a profile assigned to the Device Group and Template administrator role, the Access Control tab appears. On this tab, you define access to device groups, templates, and device context. The definitions for these fields match those described in “Specifying Panorama Access Domains for Administrators”.
Password Profile	Select the password profile, if applicable. To create a new password profile, see “ Defining Password Profiles ”.



On the Panorama Administrators page, the **Locked User** column displays a lock icon if an account is locked out. The superuser or the Panorama administrator can click the icon to unlock the account.

Specifying Panorama Access Domains for Administrators

► *Panorama > Access Domain*

Use the **Access Domain** page to specify domains for role-based administrators who have access to device groups and templates. Adding a device group to an access domain allows you to manage policies and objects for that device group. Adding an individual firewall to an access domain allows you to switch into the device context for that firewall.

The access domain is linked to RADIUS vendor-specific attributes (VSAs) and is supported only if a RADIUS server is used for administrator authentication. If RADIUS is not used, the access domain settings on this page are ignored. For information on using VSAs, see the Knowledge Point on the support portal.



The Access Domain can be mapped via RADIUS VSA using the following attribute: "PaloAlto-Panorama-Admin-Access-Domain = <AccessDomainName>".

Table 228. Access Domain Settings

Field	Description
Name	Enter a name for the access domain (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.
Device Groups	Click Add to specify pre-defined device groups to include in the access domain.
Device Context	Select the firewall(s) that the administrator can do a context switch to in order to allow local configuration edits.
Templates	Click Add to specify pre-defined templates to include in the access domain.

Committing your Changes in Panorama

To commit Panorama configuration changes click the **Commit** icon to bring up the commit dialog box. This dialog box allows you to commit specific areas of the Panorama environment, see Figure 18.

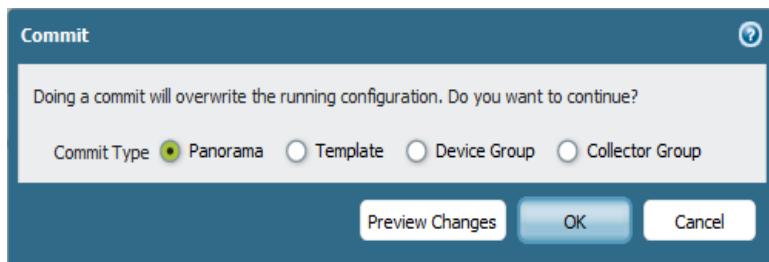


Figure 18. Panorama Commit Dialog Box

The following options are available in the commit dialog box:



You must commit changes to Panorama before committing changes to managed firewalls or managed collectors.

- **Commit Type**—Choose the commit type:
 - **Panorama**—Commit the current candidate configuration for Panorama.
 - **Template**—Commit template changes from Panorama to the selected firewalls. When committing templates, you can select a subset of firewalls if desired.
 - **Device Group**—Commit firewall configuration changes from Panorama to the selected firewall/virtual system(s).
 - **Collector Group**—Only commit changes to Collector Groups. This will commit changes made in the **Panorama > Collector Groups** page and will apply those changes to the Log Collectors.
- **Include Device and Network Templates**—This option is available when committing a Device Group from Panorama and is a combo operation that will include both the device and network template changes. The template that will be applied to the firewall is the template that the firewall belongs to as defined in **Panorama > Templates**. You can also select Commit Type Template to commit templates to firewalls.
- **Force Template Values**—When doing a Commit Type **Template**, you can select this option to remove objects on the selected firewalls or virtual systems that have been overridden by the local configuration. When doing a Commit Type **Device Group**, you need to also select the **Include Device and Network Templates** check box since overriding can only occur for template pushed configuration options. This will cause the overridden objects to inherit settings from the template. See “[Overriding Template Settings](#)”.
- **Merge with Candidate Config**—Choose this option to cause the firewall to include its local candidate configuration when the commit is invoked from Panorama. If this option is not checked, the firewall local candidate configuration is not included.
It is important to leave this option unchecked when you have local administrators making changes on a firewall and you don't want to include their changes when pushing a configuration from Panorama.
- **Preview Changes**—If the **Commit Type** is **Panorama**, you can compare the candidate configuration to the running configuration. Use the **Lines of Context** drop-down to specify the number of lines—from the compared configuration files—to display before and after the highlighted differences. If you select **All**, the results include the entire configuration files. Changes are color-coded based on settings that you and other administrators added (green), modified (yellow), or deleted (red) since the last commit. The **Panorama > Config Audit** feature performs the same function (see “[Comparing Configuration Files](#)”).



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

After the commit is complete, you will see a “Commit succeeded” messages, if there are warning messages, you will see “Commit succeeded with warnings”. To view warnings, navigate to **Panorama > Managed Devices** and see the **Last Commit State** column and click the text to view details.

Templates

► *Panorama > Templates*

Templates allow you to deploy a common-base configuration to multiple firewalls that require similar settings. Templates can be used to manage configuration options based on the **Device** and **Network** tabs. When managing firewall configuration with Panorama, you can use a combination of **Device Group** configuration (to manage shared policies and objects) settings and **Templates** settings (to apply device and network settings), but these features are managed separately because of the differences in what can be configured.

To configure Panorama templates, click **Add** to add a template and then add firewalls to it. After the first template is created, the **Template** drop-down menu displays in the **Device** and **Network** tabs. Select the desired template from the **Template** drop-down menu and configure device and network settings for the selected template.

Table 229 Template Settings (Panorama)

Field	Description
Name	<p>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.</p> <p>This name will appear in the Device and Network tab in the Template drop-down menu. When selecting a template from one of these tabs, the settings that are modified will only apply to the selected template.</p>
Description	Enter a description for the template.
Virtual Systems	<p>Select the check box if the template will be used on firewalls with multiple virtual systems. When defining template settings for multi-virtual system firewalls, you need to configure settings for each virtual system on the firewall.</p> <p>Note: A template enabled for firewalls with multi-virtual systems (multi-vsyst) cannot be pushed to firewalls with a single virtual system. When you upgrade your Panorama server to v5.0 and later, by default templates are created for configurations relating to the Network and Device tabs. If, for example, you have defined a server profile for the managed firewall(s), a template is automatically generated for the server profile. This auto-generated template is enabled for multiple virtual systems. To prevent a commit failure, make sure to clear the Virtual Systems check box before you push the template to a firewall that is not multi-vsyst capable or if the multi-vsyst capability is disabled on the firewall.</p>
Operational Mode	<p>Specify the operational mode for the firewalls to which the template will be applied. The default is normal; change to cc or fips, as required. The template commit will fail if there is a mismatch in the operational mode specified on the template with what is enabled on the firewalls included in the template: normal, fips, or cc.</p> <p><i>You must configure the operational mode locally on each firewall. Operational modes such as multi-vsyst mode, FIPS mode, or CC mode cannot be enabled using templates.</i></p>

Table 229 Template Settings (Panorama)

Field	Description
VPN Disable Mode	Selecting this check box will hide all VPN related options in the Device and Network tabs. The ability to install GlobalProtect Portal or Gateway licenses is also disabled in this mode. Note: This option is designed for countries that do not allow VPN connectivity. Palo Alto Networks hardware models that have the -NV indicator in the model name are hard coded to not allow VPN configurations, so this option should be used when creating templates for these models.
Devices	Select the check box for each firewall that you want to add to the template. Click OK to save the changes to the template. Use the filters to refine the list of firewalls that display. By default, the filter displays the entire list of managed firewalls grouped by Device Groups , Platforms , Tags ; it also displays the numerical value of the total number of managed firewalls and when you select the check box for your filtering criteria, it displays the number of firewalls in your selected criteria as a fraction of the total number of managed firewalls. Note: Adding a new firewall to a device group will not automatically add it to a template. To add a firewall to the template you must select the firewall and Commit the change to Panorama and the Template .
Group HA Peers	Select the check box to group firewalls in high availability (HA) mode together. This option allows you to easily identify firewalls that are in HA mode. When pushing shared policies, you can push to the grouped pair, instead of each firewall individually. Also, when adding a new firewall in Managed Devices, if they are in HA mode, both firewalls will be displayed together, so you can add both firewalls. When viewing an HA pair, if the configuration does not match a warning indicator will appear. You will also see an indicator if the HA firewalls are in different device groups. This option is also independent for each section, so enabling and disabling in one area, will not enable/disable for all areas. The Group HA Peers option is present in the following Panorama areas: <ul style="list-style-type: none">• Managed Devices• Templates• Device Groups• Policies tab (Target tab for all policy types)• Commit dialog

After the template is configured, you must commit your changes to Panorama and to the Templates; when you commit your changes, the configuration changes are pushed to the managed firewalls that are assigned to the template. For information on committing your changes to Panorama, see “[Committing your Changes in Panorama](#)”.

Overriding Template Settings

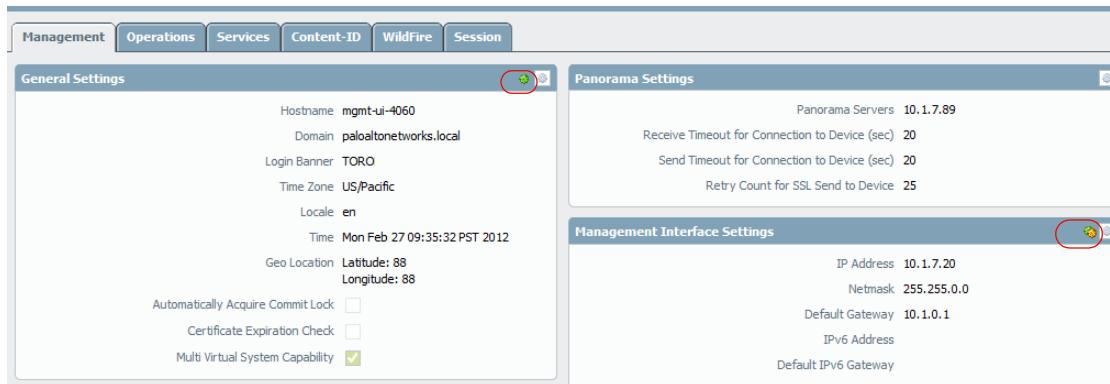
When you apply a template to control device and network settings on a firewall, you may want to override some of those settings and have them controlled by the local firewall configuration. Example, you can deploy a base configuration to a global group of firewalls, but configure specific time zones settings directly on the firewalls based on their location using an override.

To override device and network setting applied by a template, you simply change to the firewall context, or access the firewall directly, navigate to the desired setting and then click the **Override** button. The setting will be copied to the local configuration of the firewall and will no longer be controlled by the template. You can also revert the change by clicking the **Restore** button and the setting will once again be inherited from the template. When doing a commit from Panorama to a managed firewall that contains overrides, you can select the **Force Template Values** check box to have Panorama templates take over any overridden objects.

When overriding **Device > Setup and Device > High Availability** settings, the overrides are for individual values and parameters inside of configuration trees, and are not applied to an entire tree configuration. This includes items such as DNS servers, Management IP, or NTP server settings. For items such as interfaces and RADIUS server profiles, you apply overrides to the entire object, not internal values.

To identify settings that have templates applied, you will see the following indicators as shown in Figure 19:

Figure 19. Template Indicators



The single green icon indicates that a template has been applied and there are no overrides. The green and orange icon indicates that a template has been applied and some settings have been overridden.

Deleting Templates

To delete a template, select the template and click **Delete**.

Deleting the template or removing a firewall from a template will not delete the values that have been pushed to the managed firewall. When you remove a firewall from a template, new updates are no longer pushed to the managed firewall.

To disable a template on the local firewall. On the managed firewall, navigate to **Device > Setup > Management** tab, then edit the **Panorama Settings** page and click the **Disable Device and Network Template** button.

Logging and Reporting

Panorama performs two functions: configuration (of firewalls and Panorama itself) and log collection.

To facilitate scalability in large deployments, you can use the M-100 appliance to separate the management and log collection functions on Panorama. The M-100 appliance provides a comprehensive log collection solution for Palo Alto Networks firewalls. This helps offload the traffic intensive log collection process from your Panorama management server; once deployed, you can configure each firewall to send logs to an M-100 configured as a log collector. For more information on deploying a distributed log collection architecture, and for configuring and managing the log collectors using the Panorama server, see the [Panorama Administrator's Guide](#).

The Panorama logs and reports —ACC, AppScope, PDF Reports, and Logs viewer— provide information about user activity in the managed network. To view user/network activity on Panorama, you do not need to configure explicit log forwarding. Log forwarding is required for long term log storage and for generating reports using logs stored locally in Panorama. If log forwarding is enabled, by default logs are buffered on the firewall and sent at a predefined interval to Panorama.

The ACC tab in Panorama, by default displays information stored locally on Panorama. You can however, change the data source so that Panorama accesses information from the connected firewalls; all the tables pull information dynamically and display an aggregated view of the traffic on your network.

You can generate and schedule custom reports on Panorama. For scheduled predefined and custom reports, report statistics are aggregated every 15 minutes and are forwarded to Panorama on an hourly basis.

Enable Log Forwarding

► *Panorama > Log Settings*

Use this page to enable log forwarding from Panorama. Panorama can aggregate logs and forward it to the configured destinations in the form of SNMP traps, syslog messages, and email notifications.

If you have not set up server profiles to define where to send the logs —the destination for the SNMP trap, access to the syslog and/or email server— see “[Configuring SNMP Trap Destinations](#)”; “[Configuring Syslog Servers](#)”; “[Configuring Email Notification Settings](#)”.

The following table describes the logs and log forwarding options.

Table 230. Log Settings

Field	Description
System <i>On the Panorama virtual machine, use to forward system logs aggregated from the managed firewalls and the managed collectors, as well as the local Panorama logs.</i> <i>On the M-100 appliance in Panorama mode, use to forward local Panorama logs and logs from managed collectors. To forward system logs from the managed firewalls, use the Device Log Forwarding subtab on the Panorama > Collector Groups tab.</i>	The severity indicates the urgency and impact of the system event: Critical: Notifies a failure and indicates 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, such as dropped connections with external firewalls, 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 upgrades. Low: Indication of something that might be a problem or is likely to become a problem such as user password changes. Informational: Requires no attention; provides useful information during normal operation of the system. Any configuration change and all other events not covered by the other severity levels. Click the link for the severity, and select the check boxes for each option that you would like to enable. Remove all allows you to reset your choices to the defaults.
Config <i>On the Panorama virtual machine, use to forward configuration logs aggregated from the managed firewalls and the managed collectors, as well as the local Panorama logs.</i> <i>On the M-100 appliance in Panorama mode, use to forward local Panorama logs and logs from managed collectors. To forward config logs from the managed firewalls, use the Device Log Forwarding subtab on the Panorama > Collector Groups tab.</i>	Select the check boxes for each option that you would like to enable. SNMP Trap, Email, and Syslog.
HIP Match (Only on the Panorama virtual appliance.) <i>On the M-100 appliance in Panorama mode, to forward HIP Match logs from the managed firewalls, use the Device Log Forwarding subtab on the Panorama > Collector Groups tab.</i>	The HIP match log lists the host information profile (HIP) match requests for GlobalProtect. Select the check boxes for each option that you would like to enable—SNMP Trap, Email, and Syslog.

Table 230. Log Settings (Continued)

Field	Description
Traffic (Only on the Panorama virtual appliance.) <i>On the M-100 appliance in Panorama mode, to forward HIP Match logs from the managed firewalls, use the Device Log Forwarding subtab on the Panorama > Collector Groups tab.</i>	Select the check boxes for each option that you would like to enable—SNMP Trap, Email, and Syslog.
Threat (Only on the Panorama virtual appliance.) <i>On the M-100 appliance in Panorama mode, to forward HIP Match logs from the managed firewalls, use the Device Log Forwarding subtab on the Panorama > Collector Groups tab.</i>	<p>Click the link for the severity, and select the check boxes for each option that you would like to enable notification.</p> <p>Severity Description</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Low—Warning-level threats that have very little impact on an organization's infrastructure. They usually require local or physical system access and may often result in victim privacy or DoS issues and information leakage. Data Filtering profile matches are logged as Low.</p> <p>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.</p>
WildFire (Only on the Panorama virtual appliance.) <i>On the M-100 appliance in Panorama mode, to forward HIP Match logs from the managed firewalls, use the Device Log Forwarding subtab on the Panorama > Collector Groups tab.</i>	Files scanned by WildFire, receive a verdict of benign or malicious. Click the link for a verdict, and select the appropriate check boxes if you would like to be notified each time a verdict is given: <p>Benign—Indicates that the file is safe.</p> <p>Malicious—Indicates that the file contains malicious code.</p>

Managing Log Collectors

► *Panorama > Managed Collectors*

Use the Managed Collectors page to configure, manage, and update log collector devices.

- To add a log collector, see “[Adding a Log Collector](#)”
- To install a software update, see “[Installing a Software Update on a Collector](#)”

Adding a Log Collector

To add a log collector, click **Add** and complete the following fields

Table 231. Managed Collectors Page

Field	Description
General Tab	
Collector S/N	Enter the serial number of the log collector device.
Collector Name	<p>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.</p> <p>This name displays as the hostname of the log collector.</p>
Device Log Collection	Select the interface to use for firewall log collection. By default, the management interface (MGT) performs this function. To select Eth1 or Eth2, you must first enable and configure those interfaces (Panorama > Setup , Eth1/Eth2 Interface Settings).
Collector Group Communication	Select the interface to use for communication among log collectors. By default, the management interface (MGT) performs this function. To select Eth1 or Eth2, you must first enable and configure those interfaces (Panorama > Setup , Eth1/Eth2 Interface Settings).
Certificate for Secure Syslog	Select a certificate for secure forwarding of syslogs to an external Syslog server. The certificate must have the Certificate for Secure Syslog option selected (see “ Managing Device Certificates ”). When you assign a Syslog server profile to the Collector Group that includes this Log Collector, the Transport protocol of the server profile must be SSL (see “ Configuring Syslog Servers ”).
Panorama Server IP	Specify the IP address of the Panorama server used to manage this collector.
Panorama Server IP 2	Specify the IP address of the secondary device if the Panorama management server is in HA mode.
Domain	Enter the domain name of the log collector.
Primary DNS Server	Enter the IP address of the primary DNS server. The server is used for DNS queries from the log collector, for example, to find the Panorama server.
Secondary DNS Server	Enter the IP address a secondary DNS server to use if the primary server is unavailable (optional).
Primary NTP Server	Enter the IP address or host name of the primary NTP server, if any. If you do not use NTP servers, you can set the log collector time manually.
Secondary NTP Server	Enter the IP address or host name of secondary NTP servers to use if the primary server is unavailable (optional).
Timezone	Select the time zone of the log collector.
Latitude	Enter the latitude (-90.0 to 90.0) of the log collector that is used in the traffic and threat maps for App-Scope.
Longitude	Enter the longitude (-180.0 to 180.0) of the log collector that is used in the traffic and threat maps for App-Scope.
Authentication Tab	
Users	This field will always show admin and is used for the local CLI login name on the log collector.

Table 231. Managed Collectors Page

Field	Description
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 request password-hash password <password> 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 <password>.
Failed Attempts	Specify the number of failed login attempts (1-10) that are allowed for the CLI before the account is locked. The default 0 specifies unlimited login attempts. Limiting login attempts can help protect the Log Collector from brute force attacks. <i>Note: 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.</i>
Lockout Time (min)	Specify the number of minutes that a user is locked out (0-60 minutes) if the number of failed attempts is reached. <i>Note: 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.</i>

Management Tab

This tab only applies to the M-100 appliance, not the Panorama virtual appliance. By default, the M-100 appliance uses the management (MGT) port for configuration, log collection, and collector group communication. However, if you configure Eth1 or Eth2 for log collection and/or collector group communication, it is a best practice to define a separate subnet for the MGT interface that is more private than the Eth1 or Eth2 subnets. You define the subnet in the **Netmask** (for IPv4) or **IPv6 Address** (define a prefix) field.

Note: To complete the configuration of the management interface, you must specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway. If you commit a partial configuration (for example, you might omit the default gateway), you can only access the M-100 appliance via the console port for future configuration changes. It is recommended that you commit a complete configuration.

Speed and Duplex	Select the interface speed in Mbps (10, 100, or 1000) and the interface transmission mode full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
IP Address	If your network uses IPv4, assign an IPv4 address (default 192.168.1.1) to the management port of the log collector.
Netmask	If you assigned an IPv4 address to the management port, enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to the management port, assign an IPv4 address to the default router (it must be on the same subnet as the management port).
IPv6 Address	If your network uses IPv6, assign an IPv6 address to the management port of the log collector. To indicate the netmask, enter an IPv6 prefix length (for example, 2001:400:f00::1/64).

Table 231. Managed Collectors Page

Field	Description
IPv6 Default Gateway	If you assigned an IPv6 address to the management port, assign an IPv6 address to the default router (it must be on the same subnet as the management port).
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range 576-1500, default 1500).
Management Interface Services	Select the services you want enabled on the management interface of the log collector device: <ul style="list-style-type: none"> • SSH • Ping • SNMP (Simple Network Managed Protocol)
Permitted IP Addresses	Click Add to enter the list of IP addresses from which management is allowed for this interface.

Eth1 Tab

This tab only applies to the M-100 appliance, not the Panorama virtual appliance. The tab is only available if you configured Eth1 in the Panorama management settings (**Panorama > Setup > Management**, Eth1 Interface Settings).

Note: You cannot commit the Eth1 configuration unless you specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway.

Eth1	Select the check box to enable this interface.
Speed and Duplex	Select the interface speed in Mbps (10, 100, or 1000) and the interface transmission mode full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
IP Address	If your network uses IPv4, assign an IPv4 address to Eth1.
Netmask	If you assigned an IPv4 address to Eth1, enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to Eth1, assign an IPv4 address to the default router (it must be on the same subnet as Eth1).
IPv6 Address	If your network uses IPv6, assign an IPv6 address to Eth1. To indicate the netmask, enter an IPv6 prefix length (for example, 2001:400:f00:1/64).
IPv6 Default Gateway	If you assigned an IPv6 address to Eth1, assign an IPv6 address to the default router (it must be on the same subnet as Eth1).
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range 576-1500, default 1500).
Ping	Select the check box if you want to enable Ping on the Eth1 interface.
Permitted IP Addresses	Click Add to enter the list of IP addresses from which management is allowed for this interface.

Eth2 Tab

This tab only applies to the M-100 appliance, not the Panorama virtual appliance. The tab is only available if you configured Eth2 in the Panorama management settings (**Panorama > Setup > Management**, Eth2 Interface Settings).

Note: You cannot commit the Eth2 configuration unless you specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway.

Eth2	Select the check box to enable this interface.
------	--

Table 231. Managed Collectors Page

Field	Description
Speed and Duplex	Select the interface speed in Mbps (10, 100, or 1000) and the interface transmission mode full-duplex (Full), half-duplex (Half), or negotiated automatically (Auto).
IP Address	If your network uses IPv4, assign an IPv4 address to Eth2.
Netmask	If you assigned an IPv4 address to Eth2, enter a network mask (for example, 255.255.255.0).
Default Gateway	If you assigned an IPv4 address to Eth2, assign an IPv4 address to the default router (it must be on the same subnet as Eth2).
IPv6 Address	If your network uses IPv6, assign an IPv6 address to Eth2. To indicate the netmask, enter an IPv6 prefix length (for example, 2001:400:f00::1/64).
IPv6 Default Gateway	If you assigned an IPv6 address to Eth2, assign an IPv6 address to the default router (it must be on the same subnet Eth2).
MTU	Enter the maximum transmission unit (MTU) in bytes for packets sent on this interface (range 576-1500, default 1500).
Ping	Select the check box if you want to enable Ping on the Eth2 interface.
Permitted IP Addresses	Click Add to enter the list of IP addresses from which management is allowed for this interface.

Disks Tab

Click **Add** to select the RAID 1 disk pair that the Log Collector will use to store logs. You can add additional disk pairs as needed to expand the storage capacity. To make an added disk pair available to the Log Collector, select the check box. To make all the added disk pairs available, select the **Enable Disk Pair** check box.

By default, the M-100 appliance is shipped with the first RAID 1 pair enabled and installed in bays A1/A2. To increase storage capacity, you can add up to three more RAID 1 pairs in bays B1/B2, C1/C2, and D1/D2. In the software, the RAID 1 pair in bays A1/A2 is named **Disk Pair A**.

After adding log collectors, you can click the **Statistics** link for each collector to open the Collector Statistics window, which shows disk information, performance numbers for the CPU, and the average log rate (logs/second). For a better understanding of the log range you are reviewing, you can also view information on the oldest log that the collector received.

Installing a Software Update on a Collector

To install a software image on the Collector (an M-100 appliance in Log Collector mode), click **Install** and fill in the following details: .

Table 232 Software Update on a Log Collector

Field	Description
File	Select a file from the list of Uploaded or Downloaded files. You must have either downloaded an image using the Panorama > Device Deployment > Software tab or have used the Install from file option to upload a file to Panorama.
Eligible Devices	Use the filters to select the collectors on which you want to install the image.
Upload only to device (do not install)	Select this option if you would like to upload the image on the collector, but do not want to reboot it now. Until you initiate a reboot, the latest software image will not be installed.
Reboot device after install	Select this option if you want to upload and install the latest software image. A reboot will be triggered.

Defining Log Collector Groups

► *Panorama > Collector Groups*

Collector groups are used to assign Panorama managed firewalls to log collectors that will be used to offload the work of log collection that the Panorama management server would normally handle. After you establish the log collectors and configure the firewalls, PAN-OS sends the defined logs for each firewall to the log collectors. Panorama then queries the log collectors for aggregated log viewing or investigation.

To configure log collector groups, click **Add** and fill in the following details:.

Table 233. Collector Groups Settings

Field	Description
General Tab	
Name	Enter a name to identify this collector group name that will be used to group log collectors for configuration and software update purposes (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Log Storage	Indicates the current log storage quota for an individual log collector or for the collector group. If you click on the capacity text, the Log Storage Settings window will appear. From here, you can allocate storage to various log features, such as Traffic, Threat, Config, System, and Alarm. You can also click Restore Defaults to use the default log allocation settings.

Table 233. Collector Groups Settings (Continued)

Field	Description
Min Retention Period (days)	Specify the retention period in days that should be maintained across all log collectors in the group before an alert is generated. An alert violation in the form of a system log will be generated if the current date minus the oldest log is less than the defined min retention period (range 1-2000 days).
Monitoring Tab	
SNMP	<p>The SNMP option enables you to collect information about the log collectors, including: connection status, Disk drive statistics, software version, average CPU, Average log/second, and storage duration per DB type (e.g. minutes, hours, days, weeks). SNMP information is based on a per-collector group.</p> <p>Specify the SNMP settings:</p> <ul style="list-style-type: none"> • Location—Specify the location of the log collector device. • Contact—Specify an email contact for this collector. • Access Setting—Specify the SNMP version that will be used to communicate with the Panorama management server (V2c or V3). <p>If you select V3, specify the following:</p> <ul style="list-style-type: none"> – Views—Click Add and configure the following settings: <ul style="list-style-type: none"> › View—Specify a name for a view. › OID—Specify the object identifier (OID). › Option (include or exclude)—Choose whether the OID is to be included or excluded from the view. › Mask—Specify a mask value for a filter on the OID in hexadecimal format (for example, 0xf0) – Users—Click Add and configure the following settings: <ul style="list-style-type: none"> › Users—Specify a user name that will be used for authentication between the log collector and SNMP management server. › View—Specify the group of views for the user. › Authpwd—Specify the user's authentication password (minimum 8 characters). Only Secure Hash Algorithm (SHA) is supported. › Privpwd—Specify the user's encryption password (minimum 8 characters). Only Advanced Encryption Standard (AES) is supported. • SNMP Community—Specify the SNMP community string that is used by your SNMP management environment. SNMPv2c Only (default is public).
Device Log Forwarding Tab	
Collector Group Members	Click Add and, from the drop-down, select the log collector that will be part of this group. The drop-down will show all log collectors that are available in the Panorama > Managed Collectors page.

Table 233. Collector Groups Settings (Continued)

Field	Description
Devices	<p>Click Add and then click the Devices drop-down and select the managed firewall that will be part of this collector group.</p> <p>Click Add in the Collectors window and select the collector that you would like to assign this firewall for log forwarding.</p> <p>Click OK to save your changes.</p> <p>When viewing the Devices window, the Devices column will list each firewall and the Collectors column will list the assigned collector(s) for the firewall.</p> <p>The first collector you specify will be the primary collector for the firewall. If the primary collector fails, the firewall will then send logs to the secondary collector. If the secondary fails, then the tertiary collector will be used, and so on.</p> <p>Note: When you add the firewall serial number to the collector group, the firewall will start to send all logs to the collector group. To have the firewall revert back to sending logs to the Panorama manager, just remove the firewall from the collector group. This would also be required when migrating managed firewalls to a different installation of Panorama manager.</p>
Collector Log Forwarding Tab	
System	For all managed firewalls that are forwarding logs to this Collector Group, select the logs and events by severity that you want to aggregate and forward to the configured SNMP Traps, Email and Syslog servers.
Config	
HIP Match	
Traffic	If you have not already configured the server profiles for the destinations, see Panorama > Server Profiles > SNMP Trap , Panorama > Server Profiles > Email , and Panorama > Server Profiles > Syslog .
Threat	
WildFire	<i>Note: A PA-7050 firewall cannot forward logs to Panorama; you must forward the logs directly from the firewall to external servers.</i>

Generating User Activity Reports

► *Monitor > PDF Reports > User Activity Report*

The Panorama user activity report summarizes user activity across all of the managed firewalls. It is based on firewall data that has been forwarded to Panorama. See “[Managing User/Group Activity Reports](#)” for general information on creating user activity reports.

Viewing Firewall Deployment Information

► *Panorama > Device Deployment*

The **Device Deployment** tab allows you to view current deployment information on the managed firewalls. It also allows you to manage software versions and schedule updates on the managed firewalls and managed log collectors.

Table 234. Panorama Device Deployment Tabs

Field	Description
Device Deployment > Software	Lists the versions of firewall software that are available for installation on the managed firewalls and the managed log collectors.
Device Deployment > SSL VPN Client	Lists the versions of SSL VPN client software that are available for installation on the managed firewalls.
Device Deployment > GlobalProtect Client	Lists the versions of GlobalProtect client software that are available for installation on the managed firewalls.
Device Deployment > Dynamic Updates	<p>Lists the threat and application definitions that are available for use on the managed firewalls and the managed log collectors. Palo Alto Networks periodically posts updates with new or revised application definitions, information on new security threats, such as antivirus signatures, URL filtering categories, updates to GlobalProtect data, and WildFire signatures. For receiving the updates, the appropriate subscriptions are required.</p> <p>To automate the process of downloading and installing dynamic updates, see “Scheduling Dynamic Updates”.</p>
Device Deployment > Licenses	<p>Lists each managed firewall and the current license status. Each entry indicates whether the license is active ( icon) or inactive ( icon), along with the expiration date for active licenses.</p> <p>Perform either of the following functions on this page:</p> <ul style="list-style-type: none"> • Click Refresh to update the list. • Click Activate to activate a license. Select the managed firewalls for activation and enter the authentication code that Palo Alto Networks provided for the firewall.

Perform any of the following functions on the **Software**, **SSL VPN**, **GlobalProtect**, or **Dynamic Updates** tabs:

- Click **Check Now** to view the latest information on releases from Palo Alto Networks.
- Click **Release Notes** to view a description of the changes in a release.
- Click **Download** to install a new release from the download site. When the download is complete, a checkmark is displayed in the **Downloaded** column. To install a downloaded release, click **Install** next to the release.

During installation, you are asked whether to reboot when installation is complete. When the installation is complete, you will be logged out while the firewall is restarted. The firewall will be rebooted, if that option was selected.

- Click **Upload** to install or activate a release that you previously stored on your PC. Browse to select the software package, and click **Install from File**. Choose the file that you just selected from the drop-down list, and click **OK** to install the image.
- Click the **Delete** icon  to delete an outdated release.

Scheduling Dynamic Updates

► *Panorama > Device Deployment > Dynamic Updates*

Click the **Schedules** link to schedule automatic updates for managed firewalls and managed log collectors. Specify the frequency and timing for the updates and whether to download and install the update or to only download the updates.

To create a schedule, click **Add** and fill in the following details:

Table 235. Scheduling Dynamic Updates

Field	Description
Name	Enter a name to identify the scheduled job (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.
Disabled	Select the check box to disable the scheduled job.
Type	Select the dynamic update type that you would like to schedule (App and threat, antivirus, WildFire, URL Database).
Action	<p>Download Only: The scheduled update is downloaded to the selected firewalls/log collectors.</p> <p>Then, at your convenience, you can install the downloaded update by clicking the Install link in the Action column on the Dynamic Updates page.</p> <p>Download and Install: The scheduled update is download and installed; a reboot is initiated on each firewall/log collector to complete the installation.</p>
Recurrence	Select the interval at which Panorama checks in with the update server. The recurrence options vary by type of update.
Time	<p>For a Daily update, select the Time from the 24-hr clock.</p> <p>For a Weekly update, select the Day of week, and the Time from the 24-hr clock.</p>
Eligible devices	Use the filters to select the firewalls/log collectors for which you wish to schedule dynamic updates.

Scheduling Configuration Exports

► *Panorama > Scheduled Config Export*

Panorama saves a backup of running configurations from all managed firewalls in addition to its own running configuration. Use the **Scheduled Config Export** page to collect the running configurations from Panorama and all the managed firewalls, package them in one gzip file,

and schedule the package for daily delivery to an FTP server or by using Secure Copy (SCP) to transfer data securely to a remote host. The files are in XML format with file names that are based on the firewall serial numbers.

If Panorama has a high availability (HA) configuration, you must schedule configuration exports on each peer to ensure the exports continue after a failover. Panorama does not synchronize scheduled configuration exports between HA peers.

Table 236. Scheduling Configuration Bundle Exports

Field	Description
Name	Enter a name to identify the configuration bundle export job (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, hyphens, and underscores.
Description	Enter an optional description.
Enable	Select the check box to enable the export job.
Log Type	Select the log type that you would like to export (traffic, threat, URL, data, hipmatch).
Scheduled export start time (daily)	Specify the time of day to start the export (24 hour clock, format HH:MM).
Protocol	Select the protocol to use to export logs from the firewall to a remote host. You can use SCP to export logs securely, or you can use FTP, which is not a secure protocol.
Hostname	Enter the IP address or host name of the target FTP server.
Port	Enter the port number on the target server.
Path	Specify the path to the folder or directory on the FTP or SCP server where the exported information will be saved. If the configuration bundle is stored in a folder called <code>exported_config</code> within a top level folder Panorama: The syntax for the SCP server path is: <code>/Panorama/exported_config</code> The syntax for the FTP server path is: <code>//Panorama/exported_config</code>
Enable FTP Passive Mode	Select the check box to use FTP passive mode.
Username	Specify the user name on the target system.
Password	Specify the password for the user on the target system.
Confirm Password	
Test SCP server connection	Click this button to test communication between Panorama and the SCP host/server. To enable the secure transfer of data, you must verify and accept the host key of the SCP server. The connection is not established until the host key is accepted. If Panorama has an HA configuration, you must perform this verification on each HA peer so that each one accepts the host key of the SCP server.

Upgrading the Panorama Software

► *Panorama > Software*

To upgrade to a new release of Panorama software, you can view the latest versions of the Panorama software available from Palo Alto Networks, read the release notes for each version, and then select the release you want to download and install (a support license is required).

If you are upgrading the Panorama virtual machine, see the Release Notes for the recommendations on minimum system requirements and instructions on modifying the virtual machine settings after an upgrade to the 64-bit Panorama-OS v5.1.

To upgrade the Panorama software, click **Refresh** to view the latest software releases available from Palo Alto Networks. Make sure to click the **Release Notes** link next to the release and review the document for a description of the changes in a release, fixes, known issues, to review compatibility issues and any changes in default behavior.



Panorama periodically performs a file system integrity check (FSCK) to prevent corruption of the Panorama system files. This check occurs after 8 reboots or at a reboot that occurs 90 days after the last file system integrity check was executed. If Panorama is running a FSCK, you will see a warning on the web interface and SSH login screens indicating that an FSCK is in progress and you cannot log in until it completes. The time to complete this process varies by the size of the storage system; depending on the size, it can take several hours before you can log back into Panorama.

To view progress, set up console access to Panorama.

1. To install a new release:
 - a. Click **Download** next to the release to be installed. When the download is complete, a checkmark is displayed in the **Downloaded** column.
 - b. To install a downloaded release, click **Install** next to the release.
- When the installation is complete, you will be logged out while the Panorama system is restarted.
2. To delete an outdated release, click  next to the release.



Up to 5 versions of software are saved on the Panorama server. To make room for newer version downloads, the oldest version is deleted. This deletion process is automatic and cannot be manually controlled.

Register VM-Series Firewall as a Service on the NSX Manager

► *Panorama > VMware Service Manager*

To automate the provisioning of the VM-Series firewall, use the settings in this section to enable communication between the NSX Manager and Panorama. When Panorama registers the VM-Series firewall as a service on the NSX Manager, the NSX Manager has the configuration settings required to provision new VM-Series firewall(s) on each ESX(i) host in the cluster.

If you use Dynamic Address Groups, this feature allows you to secure the virtual network with minimal administrative overhead. As new virtual machines are provisioned or existing machines are modified, the changes in the virtual network are automatically provided as updates to Panorama and are then pushed from Panorama to the managed firewalls. All policy rules that reference these objects (through Dynamic Address Groups) are updated to reflect the changes in the virtual environment and ensures that security policies are consistently applied to all network resources.

Table 237. Configure the VMware Service Manager

Field	Description
Service Manager Name	Enter a name to identify the VM-Series firewall as a service. This name displays on the NSX Manager and is used to deploy VM-Series firewall on-demand. Supports up to 63 characters; use only letters, numbers, hyphens, and underscores.
Description	(optional) Enter a label to describe the purpose or function of this service.
NSX Manager URL	Specify the URL that Panorama can use to establish a connection with the NSX Manager.
NSX Manager Login	Enter the authentication credentials—username and password—configured on the NSX Manager. Panorama uses these credentials to authenticate itself and establish communication with the NSX Manager.
NSX Manager Password	
Confirm NSX Manager Password	
VM-Series OVF URL	Enter the URL (IP address or host name and path) where the NSX Manager can access the file (.ovf) to provision new VM-Series firewalls.
Authorization Code	On the purchase of the VM-Series firewall you received an order fulfillment email. Enter the authorization code provided in the order-fulfillment email.
Template	(optional) Select the template to which these VM-Series firewalls will be assigned. Templates are used to configure the settings that are required for the managed firewalls to operate on the network; they allow you to define a common base configuration using the Network and Device tabs on Panorama.
Device Group	Select the device group to which these VM-Series firewalls will be assigned. Device groups enable centralized management of policies and objects using the Policies and Objects tabs on Panorama.
Notify Device Groups	Select the device group(s) that must be notified of additions or modifications to the virtual machines deployed on the network. When configured, Panorama populates and updates changes to the registered IP addresses to the firewalls in the specified device group(s). This notification process creates context awareness and maintains application security on the network. If, for example, you have a group of hardware-based perimeter firewalls that needs to be notified when a new application or web server is deployed, this process initiates an automatic refresh of the dynamic address groups for the specified device group. And all policy rules that reference the dynamic address object now automatically include any newly deployed or modified application or web servers and can be securely enabled based on your criteria.

Table 237. Configure the VMware Service Manager (Continued)

Field	Description
Status	<p>Displays the connection status between Panorama and the NSX Manager. When the connection is successful, the status displays as:</p> <ul style="list-style-type: none"> • Registered: Panorama and the NSX Manager are in sync and the VM-Series firewall is registered as a service on the NSX Manager. <p>The unsuccessful status messages are:</p> <ul style="list-style-type: none"> • Not connected: Unable to reach/establish a network connection to the NSX Manager. • Not authorized: The access credentials (username and/or password) are incorrect. • Not registered: The service, service manager, or service profile is unavailable or was deleted on the NSX Manager. • Out of sync: The configuration settings defined on Panorama is different from what is defined on the NSX Manager. • No service / No service profile: Indicates an incomplete configuration on the NSX Manager.
Last Dynamic Update	Displays the date and time when Panorama retrieved the dynamic address group information from the NSX Manager.

Updating Information from the VMware Service Manager

The following actions can be performed on Panorama:

- **Synchronize Dynamic Objects**—Initiates a refresh of the dynamic object information from the NSX Manager. Synchronizing dynamic objects gives you the ability to maintain context on changes in the virtualized environment, and it allows you to safely enable applications by automatically updating the object references in policy.

On Panorama, you can only view the IP addresses that are dynamically registered from the NSX Manager. Panorama does not display the dynamic IP addresses that are registered directly to the firewall(s). If you are using the VM-Monitoring feature or using the XML API to register IP addresses dynamically to the firewall(s), you must log into each firewall to view the complete list of dynamic addresses that are pushed from Panorama and are locally registered to the firewall.

- **Remove VMware Service Manager**—Deletes the configuration on how to access the NSX Manager and establish communication between Panorama and the NSX Manager.

Appendix A

CUSTOM PAGES

Custom response pages allow you to notify end users of policy violations and special access conditions. Each page can include references to the user's IP address, the URL for which access is attempted, and the URL category. These parameters can also be used in links to trouble-ticketing systems.

To get the latest default response/block pages, navigate to Device > Response Pages, click a response page, click Predefined and select Export. This will save a text file of the default page. If you import a custom response/block page, that page will become the default page.

This appendix provides HTML code for the following default custom response pages:

- “Antivirus and Anti-spyware Block Page”
- “Application Block Page”
- “File Blocking Block Page”
- “SSL Decryption Opt-out Page”
- “Captive Portal Comfort Page”
- “SSL VPN Login Page”
- “SSL Certificate Revoked Notify Page”
- “URL Filtering and Category Match Block Page”
- “URL Filtering Continue and Override Page”
- “URL Filtering Safe Search Enforcement Block Page”



For information on importing and exporting custom response pages, see “[Defining Custom Response Pages](#)”.

Antivirus and Anti-spyware Block Page

```
<html>
<head>
<meta http-equiv=Content-Type content="text/html; charset=windows-1252">
<meta name=Generator content="Microsoft Word 11 (filtered)">
<title>Virus Download Blocked</title>
<style>
<!--
/* Font Definitions */
@font-face
```

```
{font-family:"Microsoft Sans Serif";
panose-1:2 11 6 4 2 2 2 2 2 4;}
/* Style Definitions */
p.MsoNormal, li.MsoNormal, div.MsoNormal
{margin:0in;
margin-bottom:.0001pt;
font-size:12.0pt;
font-family:"Times New Roman";}
h4
{margin-top:12.0pt;
margin-right:0in;
margin-bottom:3.0pt;
margin-left:0in;
page-break-after:avoid;
font-size:14.0pt;
font-family:"Times New Roman";}
p.SanSerifName, li.SanSerifName, div.SanSerifName
{margin:0in;
margin-bottom:.0001pt;
text-autospace:none;
font-size:10.0pt;
font-family:"Microsoft Sans Serif";
font-weight:bold;}
p.BoldNormal, li.BoldNormal, div.BoldNormal
{margin:0in;
margin-bottom:.0001pt;
font-size:12.0pt;
font-family:"Times New Roman";
font-weight:bold;}
span.Heading10
{color:black
font-weight:bold;}
p.SubHeading1, li.SubHeading1, div.SubHeading1
{margin-top:12.0pt;
margin-right:0in;
margin-bottom:3.0pt;
margin-left:0in;
page-break-after:avoid;
font-size:12.0pt;
font-family:"Times New Roman";
font-weight:bold;}
@page Section1
{size:8.5in 11.0in;
margin:1.0in 1.25in 1.0in 1.25in;}
div.Section1
{page:Section1;}
-->
</style>
</head>
<body lang=EN-US>
<div class=Section1>
<p class=MsoNormal>This is a test.</p>
</div>
</body>
</html>
```

Application Block Page

```
<html>
<head>
<title>Application Blocked</title>
<style>
#content{border:3px solid#aaa;background-color:#fff;margin:40;padding:40;font-family:Tahoma,Helvetica,Arial,sans-serif;font-size:12px;}
h1{font-size:20px;font-weight:bold;color:#196390;}
b{font-weight:bold;color:#196390;}
</style>
</head>
<body bgcolor="#e7e8e9">
<div id="content">
<h1>Application Blocked</h1>
<p>Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.</p>
<p><b>User:</b> <user/> </p>
<p><b>Application:</b> <appname/> </p>
</div>
</body>
</html>
```

File Blocking Block Page

```
<html>
<head>
<meta http-equiv=Content-Type content="text/html; charset=windows-1252">
<meta name=Generator content="Microsoft Word 11 (filtered)">
<title>File Download Blocked</title>
<style>
<!--
/* Font Definitions */
@font-face
    {font-family:"Microsoft Sans Serif";
    panose-1:2 11 6 4 2 2 2 2 2 4;}
/* Style Definitions */
p.MsoNormal, li.MsoNormal, div.MsoNormal
    {margin:0in;
    margin-bottom:.0001pt;
    font-size:12.0pt;
    font-family:"Times New Roman";}
h4
    {margin-top:12.0pt;
    margin-right:0in;
    margin-bottom:3.0pt;
    margin-left:0in;
    page-break-after:avoid;
    font-size:14.0pt;
    font-family:"Times New Roman";}
p.SanSerifName, li.SanSerifName, div.SanSerifName
    {margin:0in;
    margin-bottom:.0001pt;
    text-autospace:none;
    font-size:10.0pt;
    font-family:"Microsoft Sans Serif";
    font-weight:bold;}
p.BoldNormal, li.BoldNormal, div.BoldNormal
    {margin:0in;
    margin-bottom:.0001pt;
    font-size:12.0pt;
    font-family:"Times New Roman";
    font-weight:bold;}
span.Heading10
```

```

    {color:black
    font-weight:bold;}
p.SubHeading1, li.SubHeading1, div.SubHeading1
{margin-top:12.0pt;
 margin-right:0in;
 margin-bottom:3.0pt;
 margin-left:0in;
 page-break-after:avoid;
 font-size:12.0pt;
 font-family:"Times New Roman";
 font-weight:bold;}
@page Section1
{size:8.5in 11.0in;
 margin:1.0in 1.25in 1.0in 1.25in;}
div.Section1
{page:Section1;}
-->
</style>
</head>
<body lang=EN-US>
<div class=Section1>
<p class=MsoNormal>This is a test.</p>
</div>
</body>
</html>

```

SSL Decryption Opt-out Page

```

<h1>SSL Inspection</h1>
<p>In accordance with company security policy, the SSL encrypted connection
you have initiated will be temporarily unencrypted so that it can be
inspected for viruses, spyware, and other malware.</p>
<p>After the connection is inspected it will be re-encrypted and sent to its
destination. No data will be stored or made available for other purposes.</p>
<p><b>IP:</b> <url/> </p>
<p><b>Category:</b> <category/> </p>

```

Captive Portal Comfort Page

```

<h1 ALIGN=CENTER>Captive Portal</h1>
<h2 ALIGN=LEFT>In accordance with company security policy, you have to
authenticate before accessing the network.</h2>
<pan_form/>

```

SSL VPN Login Page

```

<HTML>
<HEAD>
<TITLE>Palo Alto Networks - SSL VPN</TITLE>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" type="text/css" href="/styles/
falcon_content.css?v=@@version">
<style>
td {
    font-family: Verdana, Arial, Helvetica, sans-serif;

```

```
        font-weight: bold;
        color: black; /*#FFFFFF; */
    }
    .msg {
        background-color: #ffff99;
        border-width: 2px;
        border-color: #ff0000;
        border-style: solid;
        padding-left: 20px;
        padding-right: 20px;
        max-height: 150px;
        height: expression( this.scrollHeight > 150 ? "150px" : "auto" ); /* sets
max-height for IE */
        overflow: auto;
    }
    .alert {font-weight: bold;color: red; }

</style>
</HEAD>
<BODY bgcolor="#F2F6FA">
    <table style="background-color: white; width:100%; height:45px; border-
bottom: 2px solid #888888;">
        <tr style="background-image:url(/images/logo_pan_158.gif);
background-repeat: no-repeat">
            <td align="left">&ampnbsp</td>
        </tr>
    </table>

    <div align="center">
        <h1>Palo Alto Networks - SSL VPN Portal</h1>
    </div>

    <div id="formdiv">
        <pan_form/>
    </div>
</BODY>
</HTML>
```

SSL Certificate Revoked Notify Page

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<html>

<head>
<title>Certificate Error</title>
<style>

#content {border:3px solid#aaa;background-color:#fff;margin:40;padding:40;font-family:Tahoma,Helvetica,Arial,sans-serif;font-size:12px;}

h1{font-size:20px;font-weight:bold;color:#196390; }

b{font-weight:bold;color:#196390; }

</style>
</head>

<body bgcolor="#e7e8e9">
<div id="content">
<h1>Certificate Error</h1>

<p>There is an issue with the SSL certificate of the server you are trying to contact.</p>

<p><b>Certificate Name:</b> <certname/> </p>
<p><b>IP:</b> <url/> </p>
<p><b>Issuer:</b> <issuer/> </p>
<p><b>Status:</b> <status/> </p>
<p><b>Reason:</b> <reason/> </p>
</div>
</body>
</html>
```

URL Filtering and Category Match Block Page

```
<html>
<head>
<title>Web Page Blocked</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<META HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE">
<style>
#content {border:3px solid#aaa;background-color:#fff;margin:40;padding:40;font-family:Tahoma,Helvetica,Arial,sans-serif;font-size:12px;}
    h1{font-size:20px;font-weight:bold;color:#196390; }
    b{font-weight:bold;color:#196390; }
</style>
</head>
<body bgcolor="#e7e8e9">
```

```
<div id="content">
<h1>Web Page Blocked</h1>
<p>Access to the web page you were trying to visit has been blocked in
accordance with company policy. Please contact your system administrator if
you believe this is in error.</p>
<p><b>User:</b> <user/> </p>
<p><b>URL:</b> <url/> </p>
<p><b>Category:</b> <category/> </p>
</div>
</body>
</html>
```

URL Filtering Continue and Override Page

```
<html>
<head>
<title>Web Page Blocked</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<META HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE">
<style>
#content{border:3px solid#aaa;background-
color:#fff;margin:40;padding:40;font-family:Tahoma,Helvetica,Arial,sans-
serif;font-size:12px;}
    h1{font-size:20px;font-weight:bold;color:#196390;}
    b{font-weight:bold;color:#196390;}
    form td, form input {
        font-size: 11px;
        font-weight: bold;
    }
    #formtable {
        height: 100%;
        width: 100%;
    }
    #formtd {
        vertical-align: middle;
    }
    #formdiv {
        margin-left: auto;
        margin-right: auto;
    }
</style>
<script type="text/javascript">
function pwdCheck() {
    if(document.getElementById("pwd")) {
        document.getElementById("continueText").innerHTML = "If you require
access to this page, have an administrator enter the override password
here:";
    }
}
</script>
</head>
<body bgcolor="#e7e8e9">
<div id="content">
<h1>Web Page Blocked</h1>
<p>Access to the web page you were trying to visit has been blocked in
accordance with company policy. Please contact your system administrator if
you believe this is in error.</p>
<p><b>User:</b> <user/> </p>
<p><b>URL:</b> <url/> </p>
<p><b>Category:</b> <category/> </p>

<hr>
<p id="continueText">If you feel this page has been incorrectly blocked, you
may click Continue to proceed to the page. However, this action will be
logged.</p>
<div id="formdiv">
<pan_form/>
</div>
```

```
<a href="#" onclick="history.back();return false;">Return to previous page</a>
</div>
</body>
</html>
```

URL Filtering Safe Search Enforcement Block Page

```
<html>
<head>
<script type="text/javascript">
    if (top != window) {
        top.location.replace(window.location.href);
    }
</script>
<title>Search Blocked</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<META HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE">
<style>
#content{border:3px solid#aaa;background-color:#fff;margin:40;padding:40;font-family:Tahoma,Helvetica,Arial,sans-serif;font-size:12px;}
    h1{font-size:20px;font-weight:bold;color:#196390;}
    b{font-weight:bold;color:#196390;}
</style>
</head>
<body bgcolor="#e7e8e9">
<div id="content">
<h1>Search Blocked</h1>
<p><b>User:</b> <user/> </p>
<p>Your search results have been blocked because your search settings are not in accordance with company policy. In order to continue, please update your search settings so that SafeSearch is set to strict, and try your search again.</p>
<p>For more information, please see: <a href="><ssurl/>></a></p>
<p><b>Please contact your system administrator if you believe this message is in error.</b></p>
</div>
</body>
</html>
```

Appendix B

APPLICATION CATEGORIES, SUBCATEGORIES, TECHNOLOGIES, AND CHARACTERISTICS

The appendix lists application-related categories defined by Palo Alto Networks:

- [“Application Categories and Subcategories”](#)
- [“Application Technologies”](#)
- [“Application Characteristics”](#)

The Applipedia database can also be found on the firewall in **Objects > Applications**, online at <http://apps.paloaltonetworks.com/applipedia/>, and an App is available at the Apple App Store.

Application Categories and Subcategories

The following application categories and subcategories are supported:

- business-system
 - auth-service
 - database
 - erp-crm
 - general-business
 - management
 - office-programs
 - software-update
 - storage-backup
- collaboration
 - email
 - instant-messaging
 - internet-conferencing

- social-business
- internet-utility
- social-networking
- voip-video
- web-posting
- general-internet
 - file-sharing
 - internet-utility
- media
 - audio-streaming
 - gaming
 - photo-video
- networking
 - encrypted-tunnel
 - infrastructure
 - ip-protocol
 - proxy
 - remote-access
 - routing
- unknown

Application Technologies

The following application technologies are supported.

Table 238. Application Technologies

Item	Description
browser-based	An application that relies on a web browser to function.
client-server	An application that uses a client-server model where one or more clients communicate with a server in the network.
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.

Application Characteristics

The following application characteristics are supported.

Table 239. Application Characteristics

Item	Description
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.
Transfers Files	Has the capability to transfer a file from one system to another over a network.
Tunnels Other Apps	Is able to transport other applications inside its protocol.
Used by Malware	Malware has been known to use the application for propagation, attack, or data theft, or is distributed with malware.
Vulnerability	Has publicly reported vulnerabilities.
Widely Used	Likely has more than 1,000,000 users.
Continue Scanning for Other Applications	Instructs the firewall to continue looking to see if other application signatures match. If this option is not selected, the first matching signature is reported and the firewall stops looking for additional matching applications.

Appendix C

COMMON CRITERIA/FEDERAL INFORMATION PROCESSING STANDARDS SUPPORT

You can configure the firewall to support the Common Criteria Evaluation Assurance Level 4+ (CCEAL4+) and the Federal Information Processing Standards 140-2 (FIPS 140-2), which are security certifications that ensure a standard set of security assurances and functionalities. These certifications are often required by civilian U.S. government agencies and government contractors.

Enabling CC/FIPS Mode

Use the following procedure to enable CC/FIPS mode on a software version that supports CC/FIPS. Keep in mind that when you enable CC/FIPS, the device will be reset the factory default settings; all configuration will be removed.

1. Boot the firewall into maintenance mode as follows:
 - a. Establish a serial connection with the firewall.
 - b. Reboot the device and press the **m** key on the keyboard when you see the following prompt: **Press m to boot to maint partition.**
 - c. Press any key on your keyboard when prompted to stop the automatic boot, and then select **PANOS (maint)** as the booting partition.
2. Select **Set CCEAL4 Mode** from the menu.
3. Select **Enable CCEAL4 Mode** from the menu.
4. When prompted, select **Reboot**.

After successfully switching to CC/FIPS mode, the following status displays: **CCEAL4 mode enabled successfully.** In addition, **CC** will display at all times in the status bar at the bottom of the web interface. In addition, the console port will now be available as a status output port only. In addition, the default admin login credentials change to admin/paloalto.

CC/FIPS Security Functions

When CC/FIPS is enabled, the following apply:

- To log into the firewall, the browser must be TLS 1.0 compatible.
- All passwords on the firewall must be at least six characters.
- Accounts are locked after the number of failed attempts that is configured on the **Device > Setup > Management** page. If the firewall is not in CC/FIPS mode, it can be configured so that it never locks out; however in CC/FIPS mode, and lockout time is required.
- The firewall automatically determines the appropriate level of self-testing and enforces the appropriate level of strength in encryption algorithms and cipher suites.
- Non-CC/FIPS approved algorithms are not decrypted and are thus ignored during decryption.
- When configuring IPSec, a subset of the normally available cipher suites is available.
- Self-generated and imported certificates must contain public keys that are 2048 bits (or more).
- The serial port is disabled.
- Telnet, TFTP, and HTTP management connections are unavailable.
- Surf control is not supported.
- High availability (HA) encryption is required.
- PAP authentication is disabled.

Appendix D

OPEN SOURCE LICENSES

The software included in this product contains copyrighted software that is licensed under the General Public License (GPL). A copy of that license is included in this document. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of this product by sending a money order or check for \$5 to:

Palo Alto Networks
Open Source Request
4401 Great America Parkway
Santa Clara, Ca. 95054

Some components of this product may be covered under one or more of the open source licenses listed in this appendix:

- “[Artistic License](#)”
- “[BSD](#)”
- “[GNU General Public License](#)”
- “[GNU Lesser General Public License](#)”
- “[MIT/X11](#)”
- “[OpenSSH](#)”
- “[PSF](#)”
- “[PHP](#)”
- “[Zlib](#)”

Artistic License

This document is freely plagiarized from the 'Artistic License', distributed as part of the Perl v4.0 kit by Larry Wall, which is available from most major archive sites

This documents purpose is to state the conditions under which these Packages (See definition below) viz: "Crack", the Unix Password Cracker, and "CrackLib", the Unix Password Checking library, which are held in copyright by Alec David Edward Muffett, may be copied, such that the copyright holder maintains some semblance of artistic control over the development of the packages, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

A "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification, or segments thereof. "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when AND WHY you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide separate documentation for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

- c) accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.
 - d) make other distribution arrangements with the Copyright Holder.
5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. YOU MAY NOT CHARGE A FEE FOR THIS PACKAGE ITSELF. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that YOU DO NOT ADVERTISE this package as a product of your own.
6. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.
7. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

BSD

The following copyright holders provide software under the BSD license:

- Julian Steward
- Thai Open Source Software Center Ltd
- The Regents of the University of California
- Nick Mathewson
- Niels Provos
- Dug Song
- Todd C. Miller
- University of Cambridge
- Sony Computer Science Laboratories Inc.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble:

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that see this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU Lesser General Public License

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble:

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that see this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- * a) The modified work must itself be a software library.
- * b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- * c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- * d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that see this License, so that they see the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

* a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

* b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

* c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

* d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

* e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

* a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

* b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license

would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A

FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

MIT/X11

Copyright (C) 2001-2002 Daniel Veillard. All Rights Reserved.

Copyright (C) 2001-2002 Thomas Broyer, Charlie Bozeman and Daniel Veillard. All Rights Reserved.

Copyright (C) 1998 Bjorn Reese and Daniel Stenberg.

Copyright (C) 2000 Gary Pennington and Daniel Veillard.

Copyright (C) 2001 Bjorn Reese <breese@users.sourceforge.net>

Copyright (c) 2001, 2002, 2003 Python Software Foundation

Copyright (c) 2004-2008 Paramjit Oberoi <param.cs.wisc.edu>

Copyright (c) 2007 Tim Lauridsen <tla@rasmil.dk>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSH

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1) Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

[Tatu continues]

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

-RSA is no longer included, found in the OpenSSL library

-IDEA is no longer included, its use is deprecated

-DES is now external, in the OpenSSL library

-GMP is no longer used, and instead we call BN code from OpenSSL

-Zlib is now external, in a library

-The make-ssh-known-hosts script is no longer included

-TSS has been removed

-MD5 is now external, in the OpenSSL library

-RC4 support has been replaced with ARC4 support from OpenSSL

-Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "<http://www.cs.hut.fi/crypto>".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,

REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/ OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com> <<http://www.core-sdi.com>>

3) ssh-keyscan was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <cdm@lcs.mit.edu>.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5) One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS

BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6) Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

-Markus Friedl
-Theo de Raadt
-Niels Provos
-Dug Song
-Aaron Campbell
-Damien Miller
-Kevin Steves
-Daniel Kouril
-Wesley Griffin
-Per Allansson
-Nils Nordman
-Simon Wilkinson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PSF

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 2.3 software in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 2.3 alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003 Python Software Foundation; All Rights Reserved" are retained in Python 2.3 alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python 2.3 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 2.3.
4. PSF is making Python 2.3 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 2.3 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 2.3 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 2.3, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python 2.3, Licensee agrees to be bound by the terms and conditions of this License Agreement.

PHP

The PHP License, version 3.01

Copyright (c) 1999 - 2009 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from <<http://www.php.net/software/>>".
THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see <<http://www.php.net>>.

PHP includes the Zend Engine, freely available at <<http://www.zend.com>>.

Zlib

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

- 1.The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
- 2.Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
- 3.This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

Appendix E

FIREWALL ACCESS TO EXTERNAL WEB RESOURCES

Palo Alto Networks maintains a Content Delivery Network (CDN) infrastructure for delivering content updates to the Palo Alto Networks devices. The devices access the web resources in the CDN to perform various App-ID and Content-ID functions. The following sections list what web resources are accessed by the firewall according to the feature or application they are required for:

- “Application Database”
- “Threat/Antivirus Database”
- “PAN-DB URL Filtering Database”
- “BrightCloud URL Filtering Database”
- “WildFire”

Application Database

The firewall accesses the following web resource when performing Application database updates:

- updates.paloaltonetworks.com:443

Threat/Antivirus Database

The firewall accesses the following web resources when performing Threat/Antivirus database updates:

- updates.paloaltonetworks.com:443
- downloads.paloaltonetworks.com:443

As a best practice, set the update server configuration to updates.paloaltonetworks.com. This allows the Palo Alto Networks device to receive content updates from the server closest to it in the CDN infrastructure.

If a static server is required, set the update server to access the hostname staticupdates.paloaltonetworks.com or the IP address 199.167.52.15.

PAN-DB URL Filtering Database

The firewall accesses the following web resource when performing PAN-DB URL filtering database updates and lookups:

- *urlcloud.paloaltonetworks.com

BrightCloud URL Filtering Database

The firewall accesses the following web resources when performing BrightCloud URL Filtering Database updates and lookups:

- database.brightcloud.com:443/80
- service.brightcloud.com:80

WildFire

The firewall accesses the following web resources when performing WildFire updates:

- beta.wildfire.paloaltonetworks.com:443/80
- beta-s1.wildfire.paloaltonetworks.com:443/80

Beta sites are only accessed by a firewall running a Beta release version.

- mail.wildfire.paloaltonetworks.com:25
- wildfire.paloaltonetworks.com:443/80
- wildfire.paloaltonetworks.com:443
- ca-s1.wildfire.paloaltonetworks.com:443
- va-s1.wildfire.paloaltonetworks.com:443
- eu-s1.wildfire.paloaltonetworks.com:443
- sg-s1.wildfire.paloaltonetworks.com:443
- jp-s1.wildfire.paloaltonetworks.com:443
- ca-s2.wildfire.paloaltonetworks.com:443
- va-s2.wildfire.paloaltonetworks.com:443
- eu-s2.wildfire.paloaltonetworks.com:443
- sg-s2.wildfire.paloaltonetworks.com:443
- jp-s2.wildfire.paloaltonetworks.com:443
- portal3.wildfire.paloaltonetworks.com:443/80
- ca-s3.wildfire.paloaltonetworks.com:443
- va-s3.wildfire.paloaltonetworks.com:443
- eu-s3.wildfire.paloaltonetworks.com:443
- sg-s3.wildfire.paloaltonetworks.com:443
- jp-s3.wildfire.paloaltonetworks.com:443
- wildfire.paloaltonetworks.jp:443/80
- wf1.wildfire.paloaltonetwrks.jp:443
- wf2.wildfire.paloaltonetworks.jp:443
- portal.wildfire.paloaltonetworks.jp:443/80
- wf3.wildfire.paloaltonetworks.jp:443
- wf4.wildfire.paloaltonetworks.jp:443

Index

A

access domains

- firewall 68, 73
- Panorama 405

accounts

- authentication profiles 74
- username and password requirements 71

acknowledging alarms 85

active configuration, updating 37, 44

active/active high availability 107

active/passive high availability 107

address groups, defining 262

addresses

- defining address groups 262
- defining group 262

administrator

- accounts, about 67
- authentication options 67
- page lockout 73, 392, 404
- profiles, about 67
- roles, about 67
- roles, defining 68

agent

- setting up GlobalProtect 380
- User-ID 334
- using GlobalProtect 380

alarms

- acknowledged 85
- alarm icon 85
- log settings 85
- making the icon visible 85
- thresholds 196
- unacknowledged 85
- viewing 85

allow list

- URL filtering profile 248
- wildcard patterns 247

anti-spyware profiles

- about 240
- defining 240

antivirus profiles

- defining 238

antivirus response pages 429

Application Command Center (ACC), using 297

application exception policies 287

application exceptions 239

application groups, defining 273

application override policies

- about 228

applications

- ACC page 299
- categories 270, 437
- characteristics 270, 439
- custom with application override 228
- defining 270
- defining filters 273
- defining groups 273
- details 267
- exceptions 239
- filters 266
- identifying unknown 323
- response page 431
- searching 267
- sub category 270
- subcategories 437
- technologies 439
- updating threat definitions 65, 421

applications list 299

App-Scope reports

- change monitor report 303
- network monitor report 307
- summary report 302
- threat map report 306, 309
- viewing 301

ARP entries

- on L3 subinterfaces 150
- on main L3 interfaces 136
- on VLAN interfaces 129

audit configuration 57

authentication

- LDAP 67
- local database 67
- options for administrator 67
- RADIUS 67
- remote 24, 57
- sequence 80

authentication profiles

- about 74
- Kerberos settings 79
- LDAP settings 79

RADIUS settings 78
setting up 74
authentication sequences
about 80
setting up 80

B

backing up firewall configurations 398
BGP
virtual routers 160, 161, 163, 164, 165, 168, 169
block list
URL filtering profile 247
wildcard patterns 247
blocking, file profiles 251
BrightCloud service 249
browsers, supported 21

C

candidate configuration
about 37, 44
saving and rolling back 37, 44
captive portal 74
comfort page 121, 432
configuring firewall for 339
defining policies 231
certificates
exporting 102
importing 102
clear text traffic, and QoS 381
clients
downloading and activating
GlobalProtect 378
clock, setting 24, 57
committing
changes 19
options 19
Panorama 405
comparison of configurations 57
configuration audit 57
configuration bundle exports 422
configuration log
defining remote logging 82, 85, 86
viewing 314
configuration management 37, 44
content-id settings 48
CPU utilization 297
crypto profiles 348, 349
custom group reports 320
custom reports 322
custom signatures
about 282
spyware 282
vulnerability 282

D

dashboard
firewall 296

data filtering
ACC page 299
data patterns 282
defining profiles 256
HIP matches on ACC page 299
list 299
pattern settings 257
profile settings 256, 259
profiles 256
profiles and patterns 257
viewing logs 313

data patterns

adding new 277
data filtering profiles 257
defining 282
rules 277
data protection
adding 49
changing password 49
dead peer protection 344
decoders and actions 239
decryption policy 290
defining configuration templates 424
denial of service (Dos), profiles 233
deployment, viewing information 421
device groups
adding 399

device priority, HA 395
devices
adding 396
master 400

DHCP
firewall options 190
relay 190
servers 190
settings 190, 381

Diffie-Hellman (DH) group 348
discard options, DOS profiles 199
disk utilization 297

DNS
servers 190
DNS proxy
settings 192
do not fragment (DF) 200
domain name 24

DoS
profiles 233
protection profiles 233
duplex settings 128, 140, 142, 143, 148
Duplicate Address Detection (DAD) 132, 138, 150
Dynamic Block Lists 279
dynamic updates
about 65
scheduling 422
dynamic URL timeout 48

E

editing settings on a page 18

e
 email
 scheduling report delivery 321
 email notification settings
 defining 97, 98
 in logging profiles 289
 encrypting private keys and passwords 106
 exchange mode 344
 exports
 certificates 100
 configuration bundle 422
 scheduling log 81

F

fail over 195
 features and benefits 12
 file blocking
 defining profiles 251
 profiles, defining 287
 settings 251
 file blocking page 431
 filters
 application 266, 273
 sub category 266
 FIPS 441
 firewall
 features and benefits 12
 introduction 11
 latitude and longitude 25
 navigating the user interface 20
 User-ID Agent 327
 using the web interface 17
 flood, zone protection settings 195, 196, 198, 199, 200, 201, 383
 FTP server, saving logs to 81

G

gateway
 setting up GlobalProtect 361
 getting help 18
 GlobalProtect
 downloading and activating clients 378
 response page 121
 setting up agents 380
 setting up gateways 361
 using the agent 380
 groups
 defining service 276
 device 399

H

HA1 and HA2 ports 107
 hello interval, HA 395
 help 18
 high availability
 about 107
 active/active 107
 active/passive 107, 108

configuring 107
 configuring on Panorama 394
 Panorama 394
 rules for operation and failover 107
 hold time 395
 Host Information Profile (HIP)
 HIP match log settings 85
 match log 314
 matches on ACC page 299
 setting up 377
 setting up objects 369
 host name, defining 24, 57
 HTML block pages 429

I

ICMP flood 197
 IKE
 crypto profile settings 348
 dead peer protection 344
 defining crypto profiles 348
 exchange mode 344
 IKE gateways
 setting up 343
 settings 344
 interface management profiles 193
 interfaces
 viewing status 296
 IPSec
 crypto profile settings 349
 defining crypto profiles 349
 setting up tunnels 345
 IPv6 194
 IPv6 addresses 262

K

Kerberos
 administrator roles 68
 configuring server settings 79
 knowledge base 122

L

L3 interfaces
 shared gateways 120
 latitude and longitude 25
 LDAP
 authentication 67
 configuring server settings 79
 licenses
 installing 58
 open source 443
 link groups, HA 114
 link speed and duplex 128, 140, 142, 143, 148
 link state
 setting 128, 140, 142, 143, 148
 viewing 296
 local identification 344
 lockout on Administrator's page 73, 392, 404

- log destinations
 - email 97, 98
 - SNMP traps 87
 - syslog 89
 - log exports 81
 - log forwarding
 - defining profiles 288
 - profile settings 289
 - log page links 298
 - logs 313
 - alarms 85
 - clearing 87
 - configuration settings 84
 - defining remote logging
 - for the configuration 82, 85, 86
 - for threat and traffic logs 287
 - HIP match 314
 - HIP match settings 85
 - links from ACC pages 298
 - managing 87
 - resolve hostname 311
 - saving to FTP server 81
 - scheduling exports 81
 - viewing 310
 - viewing URL filtering 313
 - loopback interfaces
 - defining 152
- M**
- management interface
 - CLI 13
 - configuring 24, 57
 - options 13
 - Panorama 13
 - web 13
 - managing configurations 37, 44
 - master device 400
 - Master Key and Diagnostics page 106
 - MD5 163
 - memory utilization 297
 - MIBs 43, 88
 - modifying settings on a page 18
 - monitor profiles 194
 - multiple virtual systems 25, 118
- N**
- NAT
 - defining policies 219
 - policies 215
 - policy examples 218
 - types 216
 - navigation 20
 - network settings 24, 57
 - next hop 156
 - NFS
 - Panorama high availability 395
 - NIS servers 190
 - NSSA (not so stub area) 161, 166
- NT LAN Manager (NTLM) 233
 - NTP servers 190
- O**
- objects
 - overview 260
 - open source licenses 443
- P**
- packet capture 313
 - accessing 313
 - capture files 323
 - configuring capture settings 323
 - profile setting 239, 245
 - taking captures 323
 - Panorama
 - access domains 405
 - adding devices 396
 - administrator account creation 403
 - administrator roles 402
 - committing 405
 - configuration bundle exports 422
 - configuring IP address 26
 - enabling access 26
 - high availability 394
 - tab 391
 - templates 407
 - templates, configuring 407
 - upgrading software 424
 - user account lockout 73, 392, 404
 - PAN-OS software
 - upgrading 63, 73, 405
 - version 296
 - passive hold time, HA 395
 - passive link state 108
 - passive/active high availability 107
 - password
 - data protection 49
 - encrypting 106
 - minimum password complexity 35
 - new 16
 - profiles 69
 - path groups, HA 396
 - PDF summary reports
 - creating 318, 321
 - designing 318
 - displaying 318
 - viewing 317
 - peer identification 344
 - polices
 - about 203
 - about NAT 215
 - about policy based forwarding 222
 - about security 208
 - data patterns 282
 - defining captive portal 231
 - defining decryption 225
 - defining NAT 219

other policy objects 260
 QoS 384
 specifying users and applications 206
 types 203
 virtual systems 117
 policy based forwarding (PBF)
 about 222
 and monitor profiles 194
 defining 222
 private key, encrypting 106
 profile groups, defining 287
 profiles
 about monitor 194
 about security 237
 anti-spyware 240
 antivirus 238
 antivirus, application exceptions 239
 antivirus, decoders and actions 239
 data filtering 256
 defining log forwarding 288
 file blocking 251, 287
 IKE crypto 348
 IKE crypto profile settings 348
 interface management 193
 IPSec crypto 349
 IPSec crypto profile settings 349
 logging 287
 QoS 383
 security groups 237, 287
 tunnel monitor 194
 URL filtering 246
 vulnerability protection 243, 246
 zone protection 59, 195, 383

Q

QoS
 classes 383, 384
 clear text traffic 381
 egress settings 383
 marking 214
 policies 384
 priority settings 383
 profiles 383
 settings 214
 tunneled traffic 381

R

RADIUS
 authentication 67
 authentication profiles 74
 defining server settings 78
 random early drop 196
 rebooting the device 24, 40, 57
 regions
 about 264
 policies 264
 regular expressions, data patterns 277
 remote authentication 24, 57

rendezvous point 179
reports
 creating custom group 320
 custom 322
 PDF summary 317
 scheduling email delivery 321
 top 50 321
 user activity 319, 420
 viewing 321
reports and logs
 custom reports 322
 identifying unknown applications 323
 using the Application Command Center 297
 using the dashboard 296
 viewing App-Scope reports 301
 viewing PDF summary reports 317
 viewing reports 321, 322
Representational State Transfer (REST) 13
requesting support 122
required fields 20
resolve hostname 311
response pages
 antivirus 121, 429
 application block 121, 431
 captive portal 121, 432
 defining 121
 file blocking 121, 431
 file blocking continue 121
 GlobalProtect portal help 121
 GlobalProtect portal login 121
 SSL certificate errors notify page 121
 SSL certificate revoked notify 434
 SSL decryption opt-out 121
 types 104, 121
 URL filtering continue and override 122
response thresholds 196, 197
roles
 about 67
 defining administrator 68
rolling back a candidate configuration 37, 44
Router Advertisement 151
routing protocols
 BGP 160, 161, 163, 164, 165, 168, 169
rules
 application exception policy 287
 security policy 208

S

Safe Search 249
saving a candidate configuration 37, 44
schedules
 configuration bundle exports 422
 defining 287, 292
security
 defining profile groups 237, 287
 profile groups 287
security policies
 about 208

- defining 208
 - security profile groups, defining 287
 - security profiles
 - about 237
 - actions 237
 - defining 287
 - security zones
 - defining 181
 - in NAT policies 220
 - sensitive information, protecting 49
 - servers
 - defining Kerberos 79
 - defining LDAP 79
 - defining RADIUS 78
 - defining syslog 89
 - service groups
 - defining 276
 - service groups, defining 276
 - services, defining 274
 - session browser 314
 - shared gateways
 - configuring 120
 - L3 interfaces 120
 - shared policy
 - master device 400
 - Shortest Path Tree (SPT) 181
 - signatures
 - custom 282
 - spyware 282
 - vulnerability 282
 - SNMP
 - community string 44
 - MIB setup 43
 - MIBs 88
 - SNMP trap destinations
 - defining 87
 - in logging profiles 289
 - software
 - upgrading 63, 73, 405, 424
 - upgrading Panorama 424
 - version 296
 - source-specific multicast (SSM) 181
 - speed, link 128, 140, 142, 143, 148
 - SSL
 - decryption policies 287
 - defining decryption policies 225
 - tech notes reference 225
 - SSL VPNs
 - about 381
 - authentication profiles 74
 - comfort page 121
 - local user database 76
 - split tunnels 364
 - sub category
 - application 270
 - filtering 266
 - support information 122
 - support information, viewing 122
 - supported browsers 21
 - SYN flood 196
 - syslog servers
 - custom syslog fields 90
 - defining 89
 - in logging profiles 289
 - system log
 - viewing 314
 - system settings 121
- T**
- tables, using in web interface 20
 - tags
 - on L2 subinterfaces 141
 - on virtual wires 126
 - threat list 299
 - threat log 290
 - defining remote logging 287
 - viewing 313
 - threats
 - ACC list 299
 - updating definitions 65, 421
 - thresholds, alarm 196
 - time
 - setting 24, 57
 - zone 24
 - traffic log 289
 - defining remote logging 287
 - viewing 313
 - Transport Layer Security (TLS) 79
 - tunnel interfaces 345
 - tunnel monitor
 - fail over 195
 - profiles 194
 - wait-recover 195
 - tunneled traffic, and QoS 381
 - tunnels
 - setting up 345
 - split for SSL VPNs 364
- U**
- UDP flood 197
 - unnumbered loopback interfaces 152
 - upgrading
 - Panorama software 424
 - PAN-OS software 63, 73, 405
 - schedules 422
 - threat and application definitions 65
 - URL filtering
 - ACC page 299
 - continue and override response page 122
 - defining profiles 246
 - dynamic categorization 249
 - list 299
 - override settings 49
 - profile settings 246
 - response pages 122
 - Safe Search 249
 - viewing log 313

user account lockout 73, 404
user database, SSL VPN 76
user interface navigation 20
User-ID Agent
 captive portal configuration 339
 configuring firewall 327
username and password requirements 71

V

version, software 296
viewing
 logs 310
 session browser 314
 session information 314
virtual routers
 configuring 155, 156, 178
 next hop 156
virtual systems
 about 117
 defining 117, 118, 119
 defining multiple 118
 enabling 25
 enabling multiple 25
 multiple 118
 policies 117
 security zones 117
virtual wire
 defining 125
VPN
 SSL, about 381
VPN tunnels
 setting up 345
vulnerability protection profiles 243, 246

W

web interface
 committing changes 19
 navigation 20
 required fields 20
 supported browsers 21
 using 17
 using tables 20
wildcard
 custom URL categories 286
 patterns for allow and block lists 247
WINS servers 190

X

XML API 13

Z

zones
 in NAT policies 220
 protection profiles 59, 195, 383