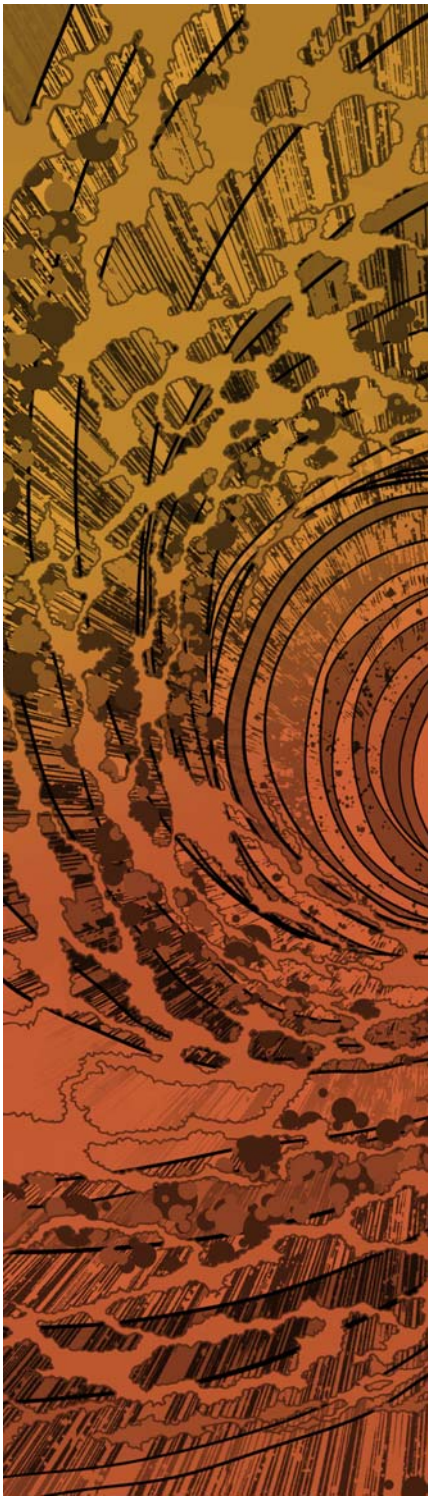


paloalto NETWORKS®

PAN-OS® New Features Guide

Version 8.0

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 describes how to use the new features introduced in PAN-OS 8.0. For additional information, refer to the following resources:

- For the most current PAN-OS and Panorama 8.0 release notes, go to https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os-release-notes.html.
- For the most current GlobalProtect Agent 4.0 Release Notes, go to https://www.paloaltonetworks.com/documentation/40/globalprotect/globalprotect-agent-rns
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.
- For information on additional capabilities included in PAN-OS 8.0 and earlier releases and for instructions on configuring the features on the firewall, refer to https://www.paloaltonetworks.com/documentation.
- For access to the knowledge base and community forums, refer to https://live.paloaltonetworks.com.

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: June 12, 2017

Table of Contents

Upgrade to PAN-OS 8.0

Upgrade/Downgrade Considerations

The following table lists the new features that have upgrade or downgrade impacts. Make sure you understand all potential changes before you upgrade to or downgrade from PAN-OS 8.0. For additional information about this release, refer to the PAN-OS 8.0 Release Notes.

- To deploy VM-Series firewalls on AWS in a high availability configuration, you must upgrade to PAN-OS 8.0.1.
- Upgrading a PA-200 or PA-500 firewall to PAN-OS 8.0 can take 30-60 minutes to complete. Ensure uninterrupted power to your firewall throughout the upgrade process.

To ensure optimal performance for all new features, download and install the latest Applications and Threats, Antivirus, and WildFire content updates (the minimum content versions required for PAN-OS 8.0 are listed in the PAN-OS 8.0 Release Notes). As a best practice, enable the firewall to download and install new content updates as they become available.

Table: PAN-OS 8.0 Upgrade/Downgrade Considerations

Feature	Upgrade Considerations	Downgrade Considerations
Hardware security modules		(PAN-OS 8.0.2 and later releases) To downgrade to a release earlier than PAN-OS 8.0.2, you must ensure that the master key is stored locally on Panorama or on the firewall, not on a hardware security module (HSM).
Log Query Acceleration on Panorama	When you upgrade Panorama and the Log Collectors to PAN-OS 8.0, logs generated from earlier PAN-OS versions will be unavailable when viewing charts on the ACC and when generating reports until you migrate the logs to the new format. See Migrate existing logs to the new log format introduced with PAN-OS 8.0.	
IKE Peer and IPSec Tunnel Capacity Increases		The firewall prevents a downgrade if the number of IKE gateways or IPSec tunnels you are using in PAN-OS 8.0 exceeds the platform limit of the release to which you are downgrading. To successfully download in this case, first delete the oversubscribed IKE peers or IPSec tunnels to the number supported in the downgraded release and then downgrade. Alternatively, restore a compatible configuration and downgrade.
VM-Series Firewall Performance Enhancements	You must increase your VM-Series firewall allocated hardware resources before upgrading to PAN-OS 8.0. For more information about new minimum hardware requirements, see VM-Series System Requirements.	Downgrading from 8.0 to an older releases returns the VM-Series models to their pre-8.0 capacities and performance levels. Downgrading the VM-50, VM-500, and VM-700 is not supported.

Feature	Upgrade Considerations	Downgrade Considerations
Authentication for External Dynamic Lists	When you create or edit an external dynamic list hosted on a web server with an HTTPS URL, you must enable Authentication for External Dynamic Lists to commit your list changes.	
Telemetry and Threat Intelligence Sharing	• The **Statistics Service** feature, available in PAN-OS 7.1 and earlier versions, is superseded by the **Telemetry and Threat Intelligence** feature in PAN-OS 8.0. Any **Statistics Service** settings you configured before upgrading are carried over to the **Telemetry and Threat Intelligence Sharing** tab. • If you enabled passive DNS monitoring on multiple firewalls through Panorama before upgrading to PAN-OS 8.0, passive DNS monitoring is disabled after you upgrade. • The service routes **Palo Alto Updates** and **WildFire Public** are merged into **Palo Alto Networks Services**.	• Any **Telemetry and Threat Intelligence** settings you configured before downgrading that are available in the **Statistics Service** feature are carried over. • If you enabled passive DNS monitoring in PAN-OS 8.0 (through the firewall or through Panorama) and downgrade to an earlier release, passive DNS monitoring is disabled. • The **Palo Alto Networks Services** service route is branched into **Palo Alto Updates** and **WildFire Public**. These two service routes will use the same settings previously configured for **Palo Alto Networks Services**.
External Dynamic List Enhancements	After you upgrade, you have the option to customize the service route that the firewall uses to retrieve an external dynamic list from the web server that hosts the list.	• If you have configured the firewall to use the **External Dynamic Lists** service route for retrieving external dynamic list updates in PAN-OS 8.0, it switches to the **Palo Alto Updates** service route upon downgrade. **External Dynamic Lists** is removed from the service route list. • Earlier PAN-OS versions support fewer external dynamic lists. Check that the total number of external dynamic lists on your firewall (both used and not used in policy) does not exceed the limit supported in the PAN-OS version to which your firewall will be downgraded. If it does exceed the limit, you will not be allowed to proceed with the downgrade until you reduce the number of external dynamic lists on the firewall to be within the limit.
Palo Alto Networks Malicious IP Address Feeds		Before downgrading to an earlier release, ensure that the Palo Alto Networks Malicious IP Address Feeds and custom external dynamic lists based on either of these feeds are not used in policy.

Feature	Upgrade Considerations	Downgrade Considerations
Globally Unique Threat IDs	• Because antivirus and DNS signatures now have globally unique IDs, the threat ID ranges that existed for these signatures in previous release versions no longer apply. If you have used antivirus and DNS threat ID ranges to build any custom logic, to create custom reports, or as part of an integration with a security information and event management (SIEM) solution, revisit those areas to see if you can leverage the new threat categories as a replacement for the ID ranges. See New Threat Categories and How to Use Them. • Antivirus and DNS threat exceptions are not migrated with the upgrade to PAN-OS 8.0. After upgrading to PAN-OS 8.0, reconfigure threat exceptions using the new, unique threat IDs (New Threat Categories and How to Use Them).	
Data Filtering Support for Data Loss Prevention (DLP) Solutions	Data pattern objects defined with both regular expression patterns and social security number and credit card patterns are separated into two separate data pattern objects following the upgrade to PAN-OS 8.0: one data pattern object contains the regular expression patterns, the other contains the social security and credit card number patterns. The separate data pattern objects continue to remain attached to data filtering profiles they were configured with before the PAN-OS 8.0 upgrade. To learn more, take a First Look at New and Updated Data Filtering Options.	
GlobalProtect tunnel-mode gateways		If you enable tunneling on a GlobalProtect internal gateway and then downgrade to an older release of PAN-OS, the gateway is removed and you must reconfigure the gateway after you downgrade. If you saved a PAN-OS 7.1 configuration that includes tunnel-mode gateways and you want to restore the configuration, downgrade the firewall from PAN-OS 8.0 to PAN-OS 7.1 first, then select and commit the saved PAN-OS 7.1 configuration.

Feature	Upgrade Considerations	Downgrade Considerations
GlobalProtect external gateways	For GlobalProtect agent configurations where you configured an external gateway with a **Manual only** priority (connections are not established automatically) and disabled **Manual** connections (users cannot manually switch to the gateway), GlobalProtect will add a **Manual only** priority rule and activate (enable) **Manual** connections when you upgrade. This allows users to manually switch to the gateway, which is required to support External Gateway Priority by Source Region.	
Authentication Policy and Multi-Factor Authentication	• Upon upgrading, the firewall changes existing Captive Portal rules to Authentication rules. Within the Authentication rules, the **Source User** defaults to **unknown** and the **Authentication Enforcement** object defaults to one of the objects that the firewall creates automatically: **default-browser-challenge**, **default-web-form**, or **default-no-captive-portal**. Each Authentication rule uses the object that is equivalent to the **Action** option in the corresponding Captive Portal rule. • The firewall does not convert System logs that it generated for authentication events before the upgrade to the new Authentication log type after upgrading. • Panorama 8.0 cannot push Authentication rules to firewalls running PAN-OS 7.1 or earlier unless the rules reference one of the predefined **Authentication Enforcement** objects. Firewalls ingest the Authentication rules as Captive Portal rules with the **Action** derived from the **Authentication Enforcement** object.	• Upon downgrading, the firewall changes Authentication rules to Captive Portal Rules with the **Action** derived from the **Authentication Enforcement** object. • Upon downgrading, the firewall discards Authentication logs.
GlobalProtect Included Access Route Capacity Enhancement	When you upgrade to Panorama to PAN-OS 8.0.2, you cannot push templates containing 200 or more GlobalProtect include access routes to firewalls running PAN-OS 8.0.1 or earlier releases. To push more than 200 access routes, you must upgrade the firewalls to PAN-OS 8.0.2. Otherwise, you must remove access routes from the template until there are 200 or fewer access routes.	Upon downgrading the firewall to PAN-OS 8.0.1 or an earlier release, a GlobalProtect configuration with more than 200 include access routes will cause a commit fail. To resolve the issue, you must remove access routes until the configuration contains 200 or fewer access routes.

Feature	Upgrade Considerations	Downgrade Considerations
Selective Log Forwarding Based on Log Attributes	• Upon upgrading, the firewall creates a separate Log Forwarding profile for each log type and severity level that had a destination in the pre-upgrade profile. Each Log Forwarding profile that the firewall creates for a severity level will have the corresponding predefined **Filter**. For example, a pre-upgrade Log Forwarding profile that specifies destinations for Threat logs with High and Critical severities will become two profiles with the **Filter** set to **(severity eq critical)** in one profile and to **(severity eq high)** in the other. • Upon upgrading, the firewall creates a match list profile for each **Device > Log Settings** entry that specifies a destination. For entries that apply to specific severity levels, the match list profiles specify a predefined filter. For example, a pre-upgrade entry that specifies destinations for System logs with medium severity will become a match list profile with the **Name** set to **system-medium** and the **Filter** set to **(severity eq medium)**.	Upon downgrading, the only log attribute that the firewall will preserve as a filter in Log Forwarding profiles and **Device > Log Settings** entries will be the log severity level.
Log Forwarding from PA-7000 Series Firewalls to Panorama	After upgrading a PA-7000 Series firewall and configuring log forwarding to Panorama, the firewall forwards only new logs. Migrating existing logs to Panorama requires a CLI command (see PA-7000 Series Firewall Log Forwarding to Panorama).	
Logging Enhancements on the Panorama Virtual Appliance	After upgrading, the Panorama virtual appliance remains in Legacy mode by default and can still support NFS log storage. However, after you switch to Panorama mode, the virtual appliance can no longer support NFS storage; you must then migrate the logs on the NFS to the Log Collectors.	Before downgrading, you must switch the Panorama virtual appliance from Panorama mode to Legacy mode. To store logs after switching the mode, you must use the old virtual disk or NFS storage that Panorama used for logging in Legacy mode.
Group-Based Reporting in Panorama	After upgrading Panorama, you must **Enable reporting and filtering on groups** in the Panorama settings (**Panorama > Setup > Management**) if you want to filter logs and generate reports based on user groups; the option is disabled by default. If you want to disable this feature for specific device groups, you must clear the **Store users and groups from Master Device** option in those device groups (**Panorama > Device Groups**); the option is enabled by default.	

Feature	Upgrade Considerations	Downgrade Considerations
User-ID Syslog Monitoring Enhancements	After upgrading, you must set the **Event Type** to **login** for every existing Syslog Parse profile assigned to syslog senders in the Server Monitoring list (**Device > User Identification > User Mapping**).	
Windows-based User-ID agent		After you uninstall the PAN-OS 8.0 Windows-based User-ID agent, perform the workaround described in Downgrade a Windows Agent from PAN-OS 8.0 before you install an earlier agent release. A PAN-OS 8.0 release of the Windows-based User-ID agent works with firewalls running a release earlier than PAN-OS 8.0.
NSX VM-Series Configuration Through Panorama	• If you are running NSX Manager 6.2.3 or earlier, create an SSL TLS Profile to allow TLS version 1.0 before upgrading from 7.1.x to 8.0. No SSL TLS profile is required when running NSX Manager 6.2.4 or later. • After upgrading Panorama from 7.1.x to 8.0, the Service Manager on Panorama goes out of sync. Executing a manual **NSX Config-sync** renames the service profile by adding the service definition name as a prefix of the service profile name. For example, a service profile called PAN_NSX_1 with a service definition called PAN-SD-1 in 7.1.x is renamed PAN-SD-1_PAN_NSX_1 in 8.0.	
Packet Buffer Protection and Zone Protection Profile		If you enable Packet Buffer Protection or you configure a Zone Protection profile with `basic evasion protection` or `strict evasion protection`, and downgrade to a PAN-OS 7.1 release, the downgrade fails with auto-commit errors. If you saved a PAN-OS 7.1 configuration before upgrading, select the PAN-OS 7.1 configuration when downgrading. This removes the Packet Buffer Protection configuration and allows downgrade to complete successfully.

Upgrade the Firewall to PAN-OS 8.0

How you upgrade to PAN-OS 8.0 depends on whether you have standalone firewalls or firewalls in a high availability (HA) configuration and, for either scenario, whether Panorama manages your firewalls. Review the PAN-OS 8.0 Release Notes and then follow the procedure specific to your configuration:

- Upgrade Firewalls Using Panorama
- Upgrade a Firewall to PAN-OS 8.0
- Upgrade an HA Firewall Pair to PAN-OS 8.0

When upgrading firewalls that you manage with Panorama or firewalls that are configured to forward content to a WF-500 appliance, you must first upgrade Panorama and its Log Collectors and upgrade the WildFire appliance before you upgrade the firewalls.

Upgrade Firewalls Using Panorama

Review the PAN-OS 8.0 Release Notes and then use the following procedure to upgrade firewalls that Panorama manages. This procedure applies to standalone firewalls and firewalls deployed in a high availability (HA) configuration.

Upgrade Firewalls Using Panorama	
Step 1 Install content and software updates on Panorama and Log Collectors. Panorama 8.0 requires the following minimum content versions: • Applications and Threats content version 655 • Antivirus content version 2137 If Panorama does not have Internet access from the management port, you can download the content updates from the Palo Alto Networks Support Portal and then manually **Upload** the updates.	1. Install content and then software updates for Panorama. 2. Deploy content and then software updates to Log Collectors. As a best practice, schedule Log Collectors to download and install the latest content updates as they are made available.

Step 2 (Log Collectors Only)
Migrate existing logs to the new log format introduced with PAN-OS 8.0.
The amount of time that Panorama takes to complete the log migration process depends on the volume of new logs being written to Panorama and the size of the log database that you are migrating. Because the log migration process is a CPU-intensive process, you can stop the migration process (**`request logdb migrate lc serial-number <ser_num> stop`**) and resume the process when the incoming log rate is lower.
	Panorama has a new log storage format in PAN-OS 8.0 to enable improved log query performance and, after upgrading, all new logs are written in the new format. Before you can generate reports on Panorama or use the ACC for visibility into traffic patterns on logs generated in earlier PAN-OS versions, you must migrate the existing logs to the new format.
	To migrate your existing logs on the Log Collectors to the new format, use the following CLI commands after you upgrade Panorama.
	1. Start migrating the logs from each Log Collector.
	`request logdb migrate lc serial-number <ser_num> start`
	2. View the log migration status to estimate the amount of time it will take to migrate all the existing logs to the new format.
	`request logdb migrate lc serial-number <ser_num> status`
	The sample output is as follows:
	`admin@FC-M100-1> request logdb migrate lc serial-number 003001000002 status`
	`Slot: all`
	`Migration State: In Progress`
	`Percent Complete: 0.04`
	`Estimated Time Remaining: 451 hour(s) 47 min(s)`
	3. To view the incoming log rate, use the following command:
	`debug log-collector log-collection-stats show incoming-logs`

Upgrade Firewalls Using Panorama (Continued)		
Step 3	Save a backup of the current configuration file on each managed firewall you plan to upgrade.  Although the firewall automatically creates a configuration backup, it is a best practice to create and externally store a backup before you upgrade.	1. Log in to Panorama and **Export Panorama and devices config bundle** (**Panorama > Setup > Operations**) to generate and export the latest configuration backup of Panorama and of each managed device. 2. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.
Step 4	Install the latest content updates on managed firewalls.  PAN-OS 8.0 requires the following minimum content versions: • Applications and Threats content release version 655 • Antivirus content version 2137  If Panorama does not have Internet access from the management port, you can download the content updates from the Palo Alto Networks Support Portal. You can then manually **Upload** the updates.	1. **Check Now** (**Panorama > Device Deployment > Dynamic Updates**) for the latest updates. If an update is available, the Action column displays a **Download** link. 2. If not already installed, **Download** the latest content version. After a successful download, the link in the Action column changes from **Download** to **Install**. 3. Click **Install**, select the firewalls on which you want to install the update, and click **OK**.  As a best practice, schedule log collectors to download and install the latest content updates as they are made available.
Step 5	Determine the software upgrade path for each firewall that you intend to upgrade to PAN-OS 8.0. You cannot skip installation of any major release versions in the path to your target PAN-OS release. For example, if you intend to upgrade from PAN-OS 6.1.13 to PAN-OS 8.0.2, you must: • Download and install PAN-OS 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0). • Download and install PAN-OS 7.1.0 and reboot. • Download PAN-OS 8.0.0. • Download and install PAN-OS 8.0.2 and reboot.	1. To access the web interface of the firewalls you intend to upgrade, use the **Context** drop-down in Panorama or log in to the firewalls directly. 2. Check which version has a check mark in the Currently Installed column for each firewall (**Device > Software**).  If upgrading more than one firewall, streamline the process by determining the upgrade paths for all firewalls you intend to upgrade before you start downloading images. 3. For each firewall, perform one of the following tasks: • If a PAN-OS 7.1 release is currently installed, skip ahead to Step 8 to upgrade the firewall to a PAN-OS 8.0 release. • If the firewall is running a release earlier than PAN-OS 7.1, proceed to Step 6 and follow the upgrade path to PAN-OS 7.1.0 before you upgrade to a PAN-OS 8.0 release.  We highly recommend that you review the known issues and changes to default behavior in the Release Notes and upgrade/downgrade considerations in the New Features Guide for each release through which you pass as part of your upgrade path.

Upgrade Firewalls Using Panorama (Continued)	
Step 6 For all firewalls you intend to upgrade to a PAN-OS 8.0 release, use the upgrade path(s) identified in Step 5 to upgrade all firewalls to a PAN-OS 7.1 release.  When upgrading more than one firewall, streamline the process by upgrading all firewalls to the same release before upgrading them all to the next release in the upgrade path. For example, for three firewalls, #1 running PAN-OS 6.1.10, #2 running PAN-OS 7.0.7, and #3 running PAN-OS 7.1.4, upgrade firewall #1 to PAN-OS 7.0.1 and then upgrade both #1 and #2 to PAN-OS 7.1.0 before you upgrade all three firewalls to PAN-OS 8.0. This is especially helpful when firewalls are unable to connect directly to the updates server and you need to download images to Panorama and distribute them to firewalls.	Repeat the following procedure until all managed firewalls that you intend to upgrade are running a PAN-OS 7.1 release—do not skip installation of any major release version in the path to your target PAN-OS 8.0 release. 1. On Panorama, **Check Now** (**Panorama > Device Deployment > Software**) for the latest updates. If an update is available, the Action column displays a **Download** link. 2. **Download** the firewall-specific file for each release in your upgrade path. You must download a separate installation file for each firewall or firewall series that you intend to upgrade. For example, to upgrade your PA-200, PA-3050, and PA-5060 firewalls to PAN-OS 7.1.0, download the `PanOS_200-7.1.0`, `PanOS_3000-7.1.0` and `PanOS_5000-7.1.0` images. After the successful download of an image, the Action column changes to **Install** for that image. 3. Perform the install tasks in Step 7 and reboot after each installation. 4. After you finish installing a new release and rebooting each firewall, perform one of the following tasks: • If the firewall is now running a PAN-OS 7.1 release, continue to Step 8. • If the firewall is still running a release earlier than PAN-OS 7.1, repeat these steps (1 through 4) for each release in the upgrade path until each firewall is running a PAN-OS 7.1 release.

Upgrade Firewalls Using Panorama (Continued)	
Step 7 Install the software update on the firewalls.  To avoid downtime when updating the software on firewalls in an HA configuration, update one peer at a time.  For firewalls in an active/active configuration, it doesn't matter which HA peer you update first. However, for an active/passive configuration, you must update the passive peer first, then suspend the active peer (to force a failover), and then update the now-passive (previously active) peer.	Perform the steps below that apply to your firewall deployment and, when finished: • If the firewalls is then running a PAN-OS 7.1 release, continue to Step 8. • If the firewall is still running a release earlier than PAN-OS 7.1, repeat Step 6 and Step 7 for each release in the upgrade path to PAN-OS 7.1. **Non-HA Firewalls** Click **Install** in the Action column for the appropriate update, select all firewalls for which you intend to update, **Reboot device after install**, and click **OK**. **Active/Active HA Firewalls** 1. Click **Install**, disable (clear) **Group HA Peers**, select either of the HA peers, **Reboot device after install**, and click **OK**. Wait for the firewall to finish rebooting before you proceed. 2. Click **Install**, disable (clear) **Group HA Peers**, select the HA peer that you didn't update in the previous step, **Reboot device after install**, and click **OK**. **Active/Passive HA Firewalls** In this example, the active firewall is named fw1 and the passive firewall is named fw2: 1. Click **Install** in the Action column for the appropriate update, disable (clear) **Group HA Peers**, select fw2, **Reboot device after install**, and click **OK**. 2. After fw2 finishes rebooting, verify on fw1 (**Dashboard** > High Availability widget) that fw2 is still the passive peer (the Local firewall state is `active` and the Peer—fw2—is `passive`). 3. Access fw1 and **Suspend local device** (**Device > High Availability > Operational Commands**). 4. Access fw2 (**Dashboard** > High Availability widget) and verify that the Local firewall state is `active` and the Peer is `suspended`. 5. Access Panorama, select **Panorama > Device Deployment > Software**, click **Install** in the Action column for the appropriate update, disable (clear) **Group HA Peers**, select fw1, **Reboot device after install**, and click **OK**. Wait for fw1 to finish rebooting before you proceed. 6. Access fw1 (**Dashboard** > High Availability widget) and verify that the Local firewall state is `passive` and the Peer (fw2) is `active`.  If you enabled preemption in Election settings (**Device > High Availability > General**), then fw1 will be reinstated as the active peer after rebooting.

Upgrade Firewalls Using Panorama (Continued)	
Step 8 Download the target PAN-OS 8.0 release image. If the firewall is not already running a PAN-OS 8.0 release, first download PAN-OS 8.0.0 (the PAN-OS 8.0 base image). Then, if upgrading to a PAN-OS 8.0 maintenance release, repeat Step 8 and Step 9 to download and install the maintenance release image.  If Panorama is unable to connect directly to the updates server, follow the procedure for deploying updates to firewalls when Panorama is not internet-connected so that you can manually download images to Panorama and then distribute the images to firewalls.	1. On Panorama, **Check Now** (**Panorama > Device Deployment > Software**) for the latest updates. If an update is available, the Action column displays a **Download** link. 2. **Download** the firewall-specific file (or files) for the release version to which you are upgrading. You must download a separate installation file for each firewall (or firewall series) that you intend to upgrade. For example, to upgrade your PA-200, PA-3050, and PA-5060 firewalls to PAN-OS 8.0.0, download the `PanOS_200-8.0.0`, `PanOS_3000-8.0.0`, and `PanOS_5000-8.0.0` images. After the successful download of an image, the Action column changes to **Install** for that image.  As a best practice, when upgrading to PAN-OS 8.0, go to Step 9 and install the PAN-OS 8.0.0 base image and reboot the firewall before you download and install a PAN-OS 8.0 maintenance release.

Upgrade Firewalls Using Panorama (Continued)	
Step 9 Install the PAN-OS 8.0 software update on the firewalls.  To avoid downtime when updating the software on firewalls in an HA configuration, update one peer at a time.  For firewalls in an active/active configuration, it doesn't matter which HA peer you update first. However, for an active/passive configuration, you must update the passive peer first, suspend the active peer (fail over), update the active peer, and then return the active peer to a functional state (fail back).	Perform the steps below that apply to your firewall deployment and, when finished, repeat Step 8 and Step 9 if you are upgrading to a PAN-OS 8.0 maintenance release.  As a best practice, when upgrading to PAN-OS 8.0, install the PAN-OS 8.0.0 base image and reboot the firewall before you download and install a PAN-OS 8.0 maintenance release. **Non-HA Firewalls** Click **Install** in the Action column for the appropriate update, select all firewalls for which you intend to update, **Reboot device after install**, and click **OK**. **Active/Active HA Firewalls** 1. Click **Install**, disable (clear) **Group HA Peers**, select either of the HA peers, **Reboot device after install**, and click **OK**. Wait for the firewall to finish rebooting before you proceed. 2. Click **Install**, disable (clear) **Group HA Peers**, select the HA peer that you didn't update in the previous step, **Reboot device after install**, and click **OK**. **Active/Passive HA Firewalls** In this example, the active firewall is named fw1 and the passive firewall is named fw2: 1. Click **Install** in the Action column for the appropriate update, clear **Group HA Peers**, select fw2, **Reboot device after install**, and click **OK**. 2. After fw2 finishes rebooting, verify on fw1 (**Dashboard** > High Availability widget) that fw2 is still the passive peer (the Local firewall state is `active` and the Peer—fw2—is `passive`). 3. Access fw1 and **Suspend local device** (**Device > High Availability > Operational Commands**). 4. Access fw2 (**Dashboard** > High Availability widget) and verify that the Local firewall state is `active` and the Peer firewall is `suspended`. 5. Access Panorama, select **Panorama > Device Deployment > Software**, click **Install** in the Action column for the appropriate update, clear **Group HA Peers**, select fw1, **Reboot device after install**, and click **OK**. Wait for fw1 to finish rebooting before you proceed. 6. Access fw1 (**Dashboard** > High Availability widget) and verify that the Local firewall state is `passive` and the Peer (fw2) is `active`.  If you enabled preemption in Election settings (**Device > High Availability > General**), then fw1 will be reinstated as the active peer after rebooting.
Step 10 Verify the software and content release version running on each managed firewall.	1. On Panorama, select **Panorama > Managed Devices**. 2. Locate the firewalls and review the content and software versions in the table.

Upgrade a Firewall to PAN-OS 8.0

Review the PAN-OS 8.0 Release Notes and then use the following procedure to upgrade a firewall not in an HA configuration to PAN-OS 8.0.

When upgrading a firewall configured to forward content to a WF-500 appliance, you must first upgrade the WildFire appliance to PAN-OS 8.0 before you upgrade the connected firewall.

Ensure the firewall is connected to a reliable power source. A loss of power during an upgrade can make the firewall unusable.

Upgrade a Firewall to PAN-OS 8.0	
Step 1 Save a backup of the current configuration file. Although the firewall automatically creates a configuration backup, it is a best practice to create and externally store a backup before you upgrade.	1. **Export named configuration snapshot** (**Device > Setup > Operations**). 2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file. 3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.
Step 2 Ensure that the firewall is running the latest content release versions. PAN-OS 8.0 requires the following minimum content versions: • Applications and Threats content release version 655 • Antivirus content version 2137 If your firewall does not have Internet access from the management port, you can download the software update from the Palo Alto Networks Support Portal. You can then manually **Upload** the image(s) to your firewall.	1. Check the **Applications** or **Applications and Threats** (**Device > Dynamic Updates**) to determine which update is currently running. 2. If the firewall is not running the minimum required update or a later version, **Check Now** to retrieve a list of available updates. 3. Locate and **Download** the content release version you intend to install. After a successful download, the link in the Action column changes from **Download** to **Install**. 4. **Install** the update. As a best practice, schedule the firewall to download and install the latest content updates as they are made available.
Step 3 Determine the upgrade path. You cannot skip installation of any major release versions in the path to your target PAN-OS release. For example, if you intend to upgrade from PAN-OS 6.1.13 to PAN-OS 8.0.2, you must: • Download and install PAN-OS 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0). • Download and install PAN-OS 7.1.0 and reboot. • Download PAN-OS 8.0.0. • Download and install PAN-OS 8.0.2 and reboot.	Check which version has a check mark in the Currently Installed column (**Device > Software**) and proceed as follows: • If a PAN-OS 7.1 release is currently installed, skip ahead to Step 5 to upgrade the firewall to a PAN-OS 8.0 release. • If the firewall is running a release earlier than PAN-OS 7.1, proceed to Step 4 and follow the upgrade path to PAN-OS 7.1.0 before you upgrade to a PAN-OS 8.0 release. We highly recommend that you review the known issues and changes to default behavior in the Release Notes and upgrade/downgrade considerations in the New Features Guide for each release through which you pass as part of your upgrade path.

Upgrade a Firewall to PAN-OS 8.0 (Continued)	
Step 4 Use the upgrade path identified in Step 3 to upgrade the firewall to a PAN-OS 7.1 release.	Repeat the following procedure until the firewall is running a PAN-OS 7.1 release—do not skip installation of any major release version in the path to your target PAN-OS 8.0 release. 1. **Check Now** (**Device > Software**) for the latest updates. If an update is available, the Action column displays a **Download** link. 2. For each release in your upgrade path, **Download** the firewall-specific file for the release version to which you are upgrading. For example, to upgrade a PA-200 firewall to PAN-OS 7.1.0, download the `PanOS_200-7.1.0` image; to upgrade a PA-3050 firewall to PAN-OS 7.1.0, download the `PanOS_3000-7.1.0` image. After a successful download, the Action column changes from **Download** to **Install** for that image. 3. **Install** the software update on the firewall, select **Reboot device after install**, and click **OK**. 4. After the firewall reboots: • If the firewall is then running a PAN-OS 7.1 release, continue to Step 5. • If the firewall is still running a release earlier than PAN-OS 7.1, repeat this step (Step 4) for each release in the upgrade path to PAN-OS 7.1.
Step 5 Install PAN-OS 8.0. If your firewall does not have Internet access from the management port, you can download the software image from the Palo Alto Networks Support Portal and then manually **Upload** it to your firewall.	1. **Check Now** (**Device > Software**) for the latest updates. 2. Locate and **Download** the version to which you intend to upgrade. If you are upgrading to a PAN-OS 8.0 maintenance release (a release other than the PAN-OS 8.0.0 base image), you must first download the PAN-OS 8.0.0 release. 3. (Optional only for base-image installation when upgrading to a maintenance release and only if you didn't manually upload the software image) After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image. For manual upgrades, you must install the base image after you download it and before you upload and install the maintenance release image. As a best practice, when upgrading to PAN-OS 8.0, install the PAN-OS 8.0.0 base image and reboot the firewall before you download and install a PAN-OS 8.0 maintenance release. 4. (Optional only for base-image installation when upgrading to a maintenance release) After the installation completes successfully, reboot using one of the following methods: • If you are prompted to reboot, click **Yes**. • If you are not prompted to reboot, go to Device Operations (**Device > Setup > Operations**) and **Reboot Device**. 5. If upgrading to a PAN-OS 8.0 maintenance release, such as PAN-OS 8.0.2, repeat steps 1 through 4 to upgrade the firewall to the maintenance release.
Step 6 Verify that the firewall is passing traffic.	Select **Monitor > Session Browser**.

Upgrade an HA Firewall Pair to PAN-OS 8.0

Review the PAN-OS 8.0 Release Notes and then use the following procedure to upgrade a pair of firewalls in a high availability (HA) configuration. This procedure applies to both active/passive and active/active configurations.

When upgrading peers in an HA configuration, you must upgrade each firewall separately. Consequently, there is a period of time when PAN-OS versions differ on the individual firewalls in the HA pair. If you have session synchronization enabled, this will continue to function during the upgrade process as long as you are upgrading from one feature release to the next consecutive feature release, such as from PAN-OS 7.1.8 to PAN-OS 8.0.2. If you are upgrading the pair from a feature release earlier than PAN-OS 7.1, session syncing between the firewalls will not work and if a failover occurs before both firewalls are running the same version of PAN-OS, then session forwarding could be impacted. If you require session continuity, then you must temporarily permit non-syn-tcp while the session table is rebuilt as described in the following procedure.

Ensure the devices are connected to a reliable power source. A loss of power during an upgrade can make the devices unusable.

Upgrade an HA Firewall Pair to PAN-OS 8.0	
Step 1 Save a backup of the current configuration file.  Although the firewall automatically creates a backup of the configuration, it is a best practice to create and externally store a backup before you upgrade.	Perform these steps on each firewall in the pair: 1. **Export named configuration snapshot** (**Device > Setup > Operations**). 2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file. 3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.
Step 2 Ensure that the firewalls are running the latest content release versions.  PAN-OS 8.0 requires the following minimum content versions: • Applications and Threats content release version 655 • Antivirus content version 2137  If your firewalls do not have Internet access from the management port, you can download the software update from the Palo Alto Networks Support Portal. You can then manually **Upload** the image(s) to your firewalls.	Perform these steps on each firewall in the pair: 1. Check the **Applications** or **Applications and Threats** (**Device > Dynamic Updates**) to determine which update is currently running. 2. If the firewall is not running the minimum required update or a later version, **Check Now** to retrieve a list of available updates. 3. Locate and **Download** the content release version you intend to install. After a successful download, the link in the Action column changes from **Download** to **Install**. 4. **Install** the update.  As a best practice, schedule your firewalls to download and install the latest content updates as they are made available.

Upgrade an HA Firewall Pair to PAN-OS 8.0 (Continued)	
Step 3 Determine the upgrade path. You cannot skip installation of any major release versions in the path to your target PAN-OS release. For example, if you intend to upgrade from PAN-OS 6.1.13 to PAN-OS 8.0.2, you must: • Download and install PAN-OS 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0). • Download and install PAN-OS 7.1.0 and reboot. • Download PAN-OS 8.0.0. • Download and install PAN-OS 8.0.2 and reboot.	Check which version has a check mark in the Currently Installed column (**Device > Software**) and proceed as follows: • If PAN-OS 7.1.0 or a later release is currently installed, continue to Step 7. • If the firewalls are running a release earlier than PAN-OS 7.1, proceed to Step 4 and follow the upgrade path to PAN-OS 7.1.0 on both peers before you upgrade to a PAN-OS 8.0 release. We highly recommend that you review the known issues and changes to default behavior in the Release Notes and upgrade/downgrade considerations in the New Features Guide for each release through which you pass as part of your upgrade path.
Step 4 Use the upgrade path identified in Step 3 to upgrade the passive device (active/passive HA configuration) or the active-secondary device (active/active HA configuration) to the next feature release in the upgrade path. If both peers are already running a PAN-OS 7.1 release, skip ahead to Step 7. If your firewall does not have Internet access from the management port, you can download the software image from the Palo Alto Networks Support Portal and then manually **Upload** it to your firewall.	Repeat all tasks in Step 4 through Step 6 for both peers in the HA configuration until both peers are running a PAN-OS 7.1 release. 1. **Check Now** (**Device > Software**) for latest updates. If an update is available, the Action column displays a **Download** link. 2. For each release in your upgrade path, **Download** the firewall-specific file for the release version to which you are upgrading. For example, to upgrade a PA-7050 firewall to PAN-OS 7.1.0, download the `PanOS_7000-7.1.0` image; to upgrade a PA-5060 firewall to PAN-OS 7.1.0, download the `PanOS_5000-7.1.0` image. After a successful download, the Action column for that image changes to **Install**. 3. After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image. 4. After the installation completes successfully, reboot using one of the following methods: • If you are prompted to reboot, click **Yes**. • If you are not prompted to reboot, go to Device Operations (**Device > Setup > Operations**) and **Reboot Device**. 5. After the device finishes rebooting, confirm (**Dashboard** > High Availability widget) that the device you just upgraded is still the passive or active-secondary peer in the HA configuration. 6. If this is the first of the two peers that you are upgrading in this HA configuration, perform one of the following tasks as appropriate and then repeat steps 1 through 5 above: • **In an active/active configuration**—Click **Install**, disable (clear) **Group HA Peers**, select the peer that you didn't update in the previous step, **Reboot device after install**, and click **OK**. • **In an active/passive configuration**—Access the peer that you didn't update in the previous steps and Suspend local device (**Device > High Availability > Operational Commands**).

Upgrade an HA Firewall Pair to PAN-OS 8.0 (Continued)		
Step 5	Suspend the active (or active-primary) firewall.	1. On the active (or active-primary) peer, **Suspend local device** (**Device > High Availability > Operational Commands**). 2. Verify (**Dashboard** > High Availability widget) that the state of the passive device changes to active. 3. Verify that the peer firewall took over as the active (or active-primary) peer and is passing traffic (**Monitor > Session Browser**). 4. (Optional—PAN-OS 6.0 and earlier releases only) If you have session synchronization enabled and you are currently running a PAN-OS version prior to 6.1.0, run the **`set session tcp-reject-non-syn no`** operational command. This will rebuild the session table so that sessions that started prior to the upgrade will continue.
Step 6	Install the same PAN-OS software update (that you installed on what was the passive or active-secondary peer in Step 4) onto the second peer (which should now be the passive or active-secondary peer after you completed the tasks in Step 5).	1. **Check Now** (**Device > Software**) for the latest updates. If an update is available, the Action column displays a **Download** link. 2. **Download** the same firewall-specific file for the release version to which you are upgrading that you most recently downloaded and installed on the HA peer in Step 4. After a successful download, the Action column changes to **Install** for that image. 3. After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image. 4. After the installation completes successfully, reboot using one of the following methods: • If you are prompted to reboot, click **Yes**. • If you are not prompted to reboot, go to Device Operations (**Device > Setup > Operations**) and **Reboot Device**. 5. Verify (**Dashboard** > High Availability widget) that the Local firewall state is `passive` and the Peer (fw2) is `active`. If you enabled preemption in Election settings (**Device > High Availability > General**), a currently passive peer will revert to `active` state when state synchronization is complete. 6. (Optional—PAN-OS 6.0 and earlier releases only) If you configured the firewall to temporarily allow non-syn-tcp traffic in order to enable the firewall to rebuild the session table in Step 7, revert back by running the **`set session tcp-reject-non-syn yes`** command. 7. Proceed to the next installation step as follows: • If the firewalls are both now running a PAN-OS 7.1 release, continue to Step 7. • If the firewalls are still running a release earlier than PAN-OS 7.1, repeat Step 4 through Step 6 for each release in the upgrade path to PAN-OS 7.1 before you continue to Step 7.

Upgrade an HA Firewall Pair to PAN-OS 8.0 (Continued)	
Step 7 Install PAN-OS 8.0 on the passive device (active/passive HA configuration) or on the active-secondary device (active/active HA configuration).  If your firewall does not have Internet access from the management port, you can download the software image from the Palo Alto Networks Support Portal and then manually **Upload** it to your firewall.	1. **Check Now** (**Device > Software**) for the latest updates. 2. Locate and **Download** the version to which you intend to upgrade. If you are upgrading to a PAN-OS 8.0 maintenance release (a release other than the PAN-OS 8.0.0 base image), you must first download the PAN-OS 8.0.0 release. 3. (Optional only for base-image installation when upgrading to a maintenance release and only if you didn't manually upload the software image) After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image.  For manual upgrades, you must install the base image after you download it and before you upload and install the maintenance release image.  As a best practice, when upgrading to PAN-OS 8.0, install the PAN-OS 8.0.0 base image and reboot the firewall before you download and install a PAN-OS 8.0 maintenance release. 4. (Optional only for base-image installation when upgrading to a maintenance release) After the installation completes successfully, reboot using one of the following methods: • If you are prompted to reboot, click **Yes**. • If you are not prompted to reboot, go to Device Operations (**Device > Setup > Operations**) and **Reboot Device**. 5. After the device finishes rebooting, confirm (**Dashboard** > High Availability widget) that the device you just upgraded is still the passive or active-secondary peer in the HA configuration. 6. If this is the first of the two peers that you are upgrading in this HA configuration, perform one of the following tasks as appropriate and then repeat steps 1 through 5 above: • **In an active/active configuration**—Click Install, disable (clear) Group HA Peers, select the peer that you didn't update in the previous step, Reboot device after install, and click OK. • **In an active/passive configuration**—Access the peer that you didn't update in the previous steps and Suspend local device (**Device > High Availability > Operational Commands**).
Step 8 Suspend the active (or active-primary) firewall.	1. On the active (or active-primary) peer, **Suspend local device** (**Device > High Availability > Operational Commands**). 2. View the High Availability widget (**Dashboard**) and verify that the state of the passive device changes to active. 3. Verify that the peer firewall took over as the active (or active-primary) peer and is passing traffic (**Monitor > Session Browser**).

Upgrade an HA Firewall Pair to PAN-OS 8.0 (Continued)	
Step 9 Install the same PAN-OS 8.0 release version (that you installed on what was the passive or active-secondary peer in Step 7) onto the second peer (which should now be the passive or active-secondary peer after you completed the tasks in Step 8).	1. **Check Now** (**Device > Software**) for the latest updates. 2. Locate and **Download** the same PAN-OS 8.0 release version that you installed on the peer in Step 7. If you are upgrading to a PAN-OS 8.0 maintenance release (a release other than the PAN-OS 8.0.0 base image), you must first download the PAN-OS 8.0.0 release. 3. (Optional only for base-image installation when upgrading to a maintenance release and only if you didn't manually upload the software image) After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image.  For manual upgrades, you must install the base image after you download it and before you upload and install the maintenance release image.  As a best practice, when upgrading to PAN-OS 8.0, install the PAN-OS 8.0.0 base image and reboot the firewall before you download and install a PAN-OS 8.0 maintenance release. 4. (Optional only for base-image installation when upgrading to a maintenance release) After the installation completes successfully, reboot using one of the following methods: • If you are prompted to reboot, click **Yes**. • If you are not prompted to reboot, go to Device Operations (**Device > Setup > Operations**) and **Reboot Device**. After the reboot, the device will not be functional until the active/active-primary device is suspended.
Step 10 Verify that the firewalls are passing traffic as expected. In an active/passive configuration, only the active peer should be passing traffic; both peers should be passing traffic in an active/active configuration.	Run the following CLI commands to confirm that the upgrade succeeded: • (Active peers only) To verify that active peers are passing traffic, run the **`show session all`** command. • To verify session synchronization, run the **`show high-availability interface ha2`** command and make sure that the Hardware Interface counters on the CPU table are increasing as follows: • In an active/passive configuration, only the active peer shows packets transmitted; the passive peer will show only packets received.  If you enabled HA2 keep-alive, the hardware interface counters on the passive peer will show both transmit and receive packets. This occurs because HA2 keep-alive is bi-directional, which means that both peers transmit HA2 keep-alive packets. • In an active/active configuration, you will see packets received and packets transmitted on both peers.

Downgrade from PAN-OS 8.0

The way you downgrade a firewall from PAN-OS 8.0 depends on whether you are downgrading to a previous feature release (where the first or second digit in the PAN-OS version changes, for example, from 8.0.2 to 7.1.7 or from 7.1.6 to 7.0.9) or downgrading to a maintenance release version within the same feature release (where the third digit in the release version changes, for example, from 8.0.2 to 8.0.0). When you downgrade from one feature release to an earlier feature release, you can migrate the configuration from the later release to accommodate new features. To migrate the PAN-OS 8.0 configuration to an earlier PAN-OS release, first restore the configuration for the feature release to which you are downgrading. You do not need to restore the configuration when you downgrade from one maintenance release to another within the same feature release.

- Downgrade a Firewall to a Previous Maintenance Release
- Downgrade a Firewall to a Previous Feature Release
- Downgrade a Windows Agent from PAN-OS 8.0

Always downgrade into a configuration that matches the software version. Unmatched software versions and configurations can result in failed downgrades or force the system into maintenance mode. This only applies to a downgrade from one feature release to another (for example 8.0.0 to 7.1.3), not to downgrades to maintenance releases within the same feature release version (for example, 7.1.7 to 7.1.2).

If you have a problem with a downgrade, you may need to enter maintenance mode and reset the device to factory default and then restore the configuration from the original config file that was exported prior to the upgrade.

Downgrade a Firewall to a Previous Maintenance Release

Because maintenance releases do not introduce new features, you can downgrade to a previous maintenance release in the same feature release without having to restore the previous configuration. A maintenance release is a release in which the third digit in the release version changes, for example a downgrade from 7.1.7 to 7.1.2 is considered a maintenance release downgrade because only the third digit in the release version is different.

Use the following procedure to downgrade to a previous maintenance release within the same feature release.

Downgrade to a Previous Maintenance Release		
Step 1	Save a backup of the current configuration file.  Although the firewall automatically creates a backup of the configuration, it is a best practice to create a backup before you downgrade and store it externally.	1. Select **Device > Setup > Operations** and **Export named configuration snapshot**. 2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file. 3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the downgrade.
Step 2	Install the previous maintenance release image.  If your firewall does not have Internet access from the management port, you can download the software update from the Palo Alto Networks Support Portal. You can then manually **Upload** it to your firewall.	1. Select **Device > Software** and **Check Now** for available images. 2. Locate the version to which you want to downgrade. If the image is not already downloaded, then **Download** it. (If the image is already downloaded, proceed to step 3.) 3. After the download completes, **Install** the image. 4. After the installation completes successfully, reboot using one of the following methods: • If you are prompted to reboot, click **Yes**. • If you are not prompted to reboot, go to Device Operations (**Device > Setup > Operations**) and **Reboot Device**.

Downgrade a Firewall to a Previous Feature Release

Use the following workflow to restore the configuration that was running before you upgraded to a different feature release. Any changes made since the upgrade are lost so it is important to back up your current configuration so you can restore those changes when you return to the newer feature release.

Downgrades from PAN-OS 8.0 to any version earlier than PAN-OS 5.0.5 is not supported because the log management subsystem has been significantly enhanced between PAN-OS 5.0 and PAN-OS 6.0. Because of the changes implemented in the log partitions, a firewall that is downgraded to PAN-OS 5.0.4 and earlier releases cannot accurately estimate the disk capacity available for storing logs and the log partition can reach maximum capacity without a user notification. Such a situation allows the log partition to reach 100% capacity, which results in a loss of logs.

Use the following procedure to downgrade to a previous feature release.

Downgrade to a Previous Feature Release	
Step 1 Save a backup of the current configuration file.  Although the firewall automatically creates a backup of the configuration, it is a best practice to create a backup before you upgrade and store it externally.	1. Select **Device > Setup > Operations** and **Export named configuration snapshot**. 2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file. 3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the downgrade.
Step 2 Install the previous feature release image.  Autosave versions are created when you upgrade to a new release.	1. Select **Device > Software** and **Check Now** for available images. 2. Locate the image to which you want to downgrade. If the image is not already downloaded, then **Download** it. (If the image is already downloaded, proceed to step 3.) 3. After the download completes, **Install** the image. 4. **Select a Config File for Downgrading**, which the firewall will load after you reboot the device. In most cases, you should select the configuration that was saved automatically when you upgraded from the release to which you are now downgrading. For example, if you are running PAN-OS 8.0 and are downgrading to PAN-OS 7.1.3, select `autosave-7.1.3`. 5. After the installation completes successfully, reboot using one of the following methods: • If you are prompted to reboot, click **Yes**. • If you are not prompted to reboot, go to Device Operations (**Device > Setup > Operations**) and **Reboot Device**.

Downgrade a Windows Agent from PAN-OS 8.0

After you uninstall the PAN-OS 8.0 Windows-based User-ID agent, perform the following steps before you install an earlier agent release.

A PAN-OS 8.0 release for the Windows-based User-ID agent works with firewalls running a release earlier than PAN-OS 8.0.

Downgrade a Windows Agent from PAN-OS 8.0	
Step 1	Open the Windows Start menu and select **Administrative Tools**.
Step 2	Select **Computer Management > Services and Applications > Services** and double-click **User-ID Agent**.
Step 3	Select **Log On**, select **This account**, and specify the username for the User-ID agent account.
Step 4	Enter the **Password** and **Confirm Password**.
Step 5	Click **OK** to save your changes. You can then install the Windows-based User-ID agent for a release earlier than PAN-OS 8.0.

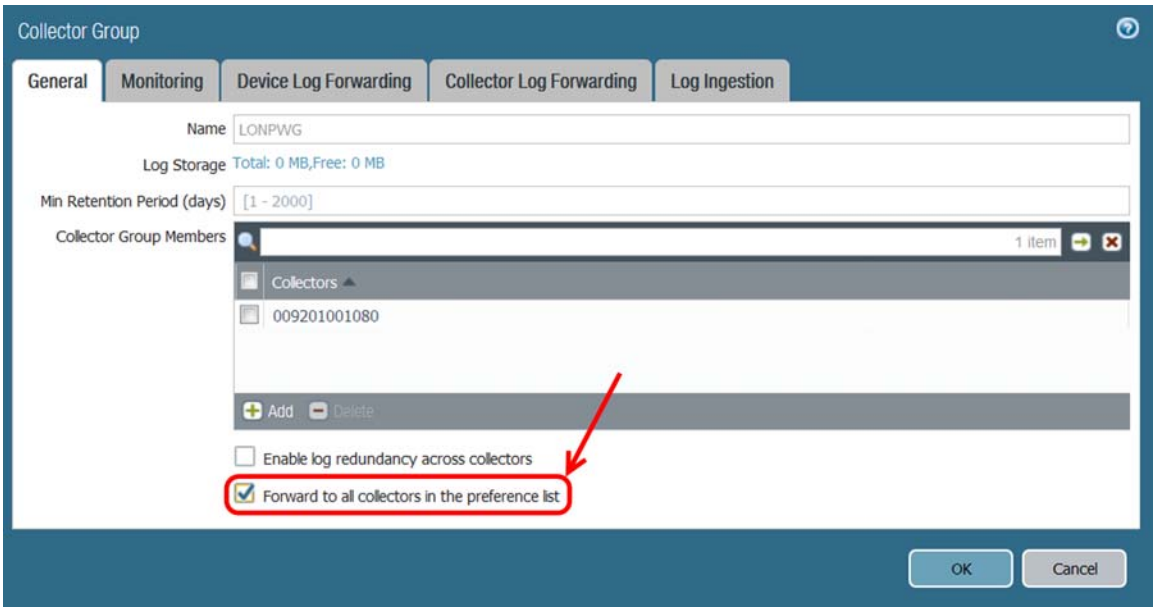
Management Features

- PA-7000 Series Firewall Log Forwarding to Panorama
- NetFlow Support for PA-7000 Series Firewalls
- Action-Oriented Log Forwarding using HTTP
- Selective Log Forwarding Based on Log Attributes
- Admin-Level Commit and Revert
- Extended SNMP Support

PA-7000 Series Firewall Log Forwarding to Panorama

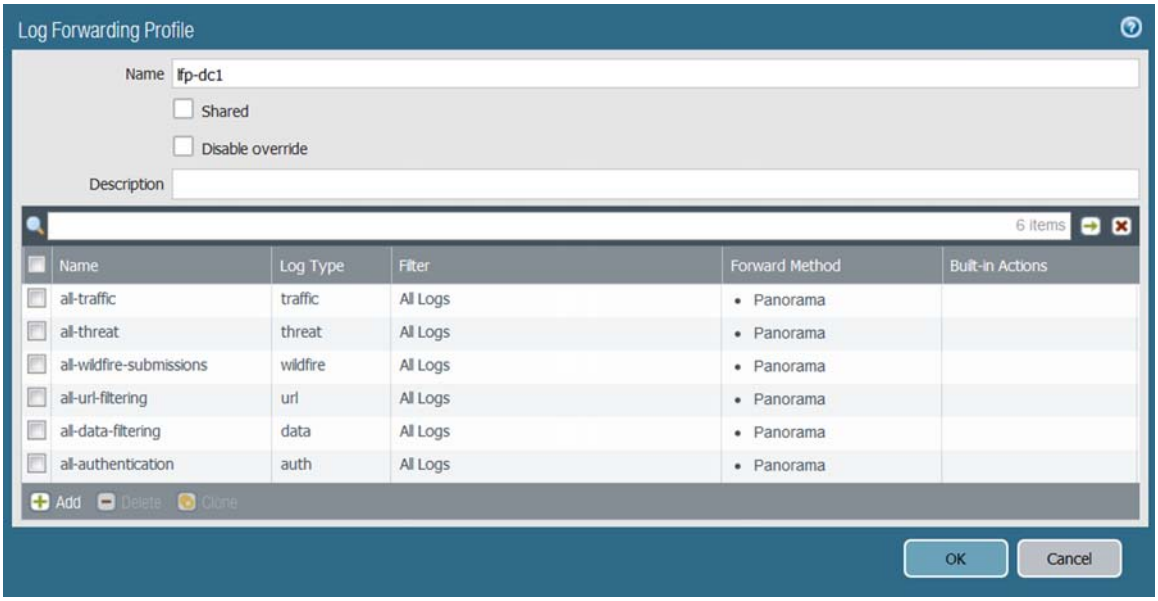
You can now forward logs from PA-7000 Series firewalls to Panorama for improved log retention, which helps you meet regulatory requirements for your industry (such as the Sarbanes-Oxely Act or HIPAA) as well as your internal log archival requirements.

The following steps describe how to configure log forwarding from a PA-7000 Series firewall that you manage from Panorama using device groups and templates.

Configure Log Forwarding from a PA-7000 Series Firewall to Panorama	
Step 1	Configure a managed collector if you need a new Log Collector to receive the firewall logs. You can also use an existing Log Collector.
Step 2	Configure a new Collector Group or edit an existing one. Assign the PA-7000 Series firewall to specific Log Collectors for log forwarding. In environments with high logging rates, you can **Forward to all collectors in the preference list** to load balance the log traffic across all Log Collectors in a Collector Group. Load balancing helps reduce bandwidth competition, which might otherwise result in dropped logs. 

Configure Log Forwarding from a PA-7000 Series Firewall to Panorama

Step 3 Select **Objects > Log Forwarding**, select the **Device Group** of the PA-7000 Series firewall, and **Add** a Log Forwarding profile to define the destinations for Traffic, Threat, WildFire Submission, URL Filtering, Data Filtering, Tunnel Inspection, or Authentication logs. **Add** one or more match list profiles for each log type you want to forward to Panorama.



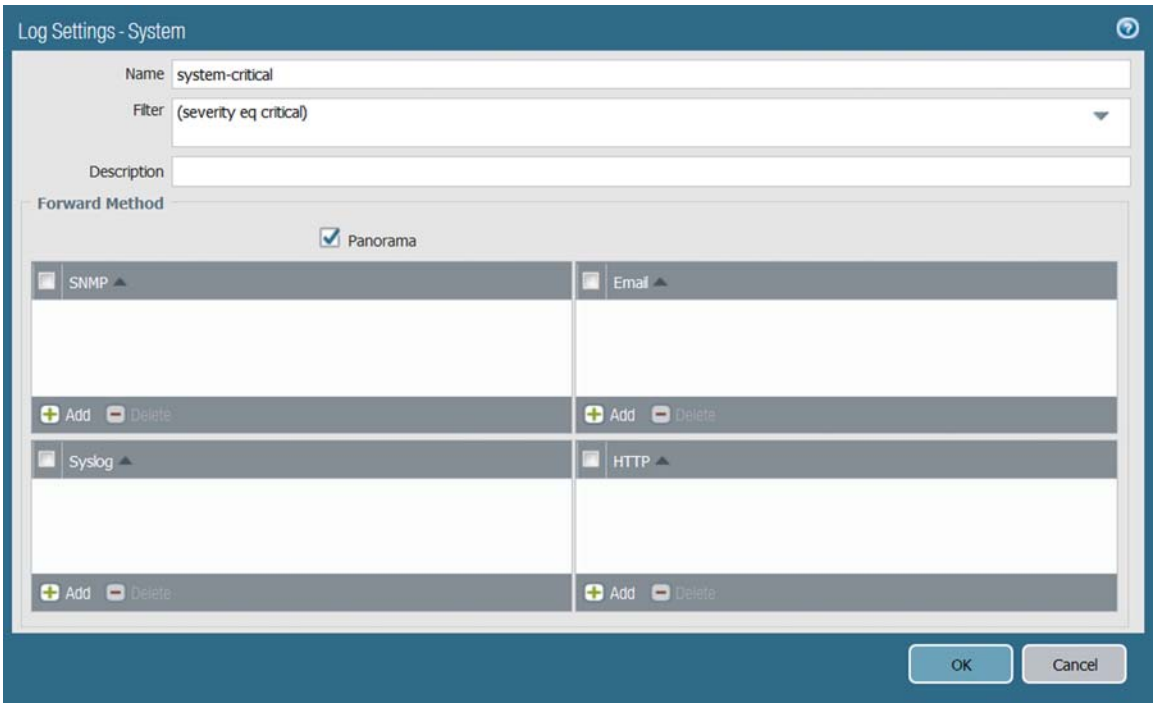
If you want to forward only certain logs to Panorama, you can configure Selective Log Forwarding Based on Log Attributes.

Step 4 Assign the Log Forwarding profile to the policy rules that trigger log generation and forwarding. Security, Authentication, and DoS Protection rules support log forwarding.

For example, to assign the profile to a Security policy pre-rule, select **Policies > Security > Pre Rules**, select the **Device Group** of the PA-7000 Series firewall, edit the rule, select **Actions**, and select the **Log Forwarding** profile.

Configure Log Forwarding from a PA-7000 Series Firewall to Panorama

Step 5 Select **Device > Log Settings**, select the **Template** to which the PA-7000 Series firewall is assigned, and **Add** one or more match list profiles to forward System, Configuration, User-ID, or HIP Match logs to Panorama.



Step 6 Select **Network > Interfaces > Ethernet**, select the **Template** to which the PA-7000 Series firewall is assigned, **Add Interface**, and configure a **Log Card** interface to perform log forwarding.

Step 7 (Optional) If you want to raise the maximum log forwarding rate from 80,000 logs/second (default) to 120,000 logs/second, select **Device > Setup > Management**, edit the Logging and Reporting Settings, select **Log Export and Reporting**, and **Enable High Speed Log Forwarding**.

If you enable this option, the firewall does not store logs locally or display them in the **Dashboard**, **ACC**, or **Monitor** tabs.

Step 8 Select **Commit > Commit and Push** to activate your changes on Panorama and push them to the device groups, templates, and Collector Groups that you modified.

Step 9 Verify your changes by logging in to the CLI of the PA-7000 Series firewall and running the following command:

```
> show logging-status
```

For successful forwarding, the output indicates that the log forwarding agent is active.

Step 10 At the firewall CLI, migrate existing logs to Panorama by entering the following command for each log type:

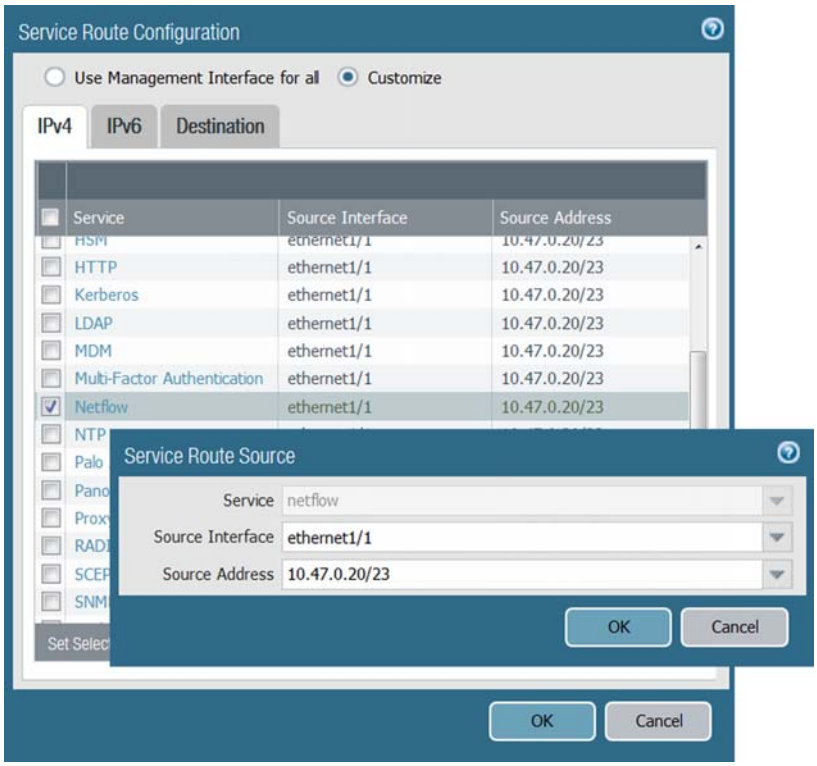
```
> request logdb migrate-to-panorama start end-time <end-time> start-time <start-time>
type <log-type>
```

This is a one-time task that you must perform after upgrading to PAN-OS 8.0.

NetFlow Support for PA-7000 Series Firewalls

PA-7000 Series firewalls now have the same ability as other Palo Alto Networks firewalls to export session-based NetFlow records to a NetFlow collector. This gives you more comprehensive visibility into how users and devices are using network resources.

Configure NetFlow Exports from the PA-7000 Series Firewall	
Step 1	Select **Device > Server Profiles > NetFlow** and **Add** a NetFlow server profile to define how the firewall connects to the NetFlow collector.
Step 2	Assign the NetFlow server profile to the firewall interfaces that convey the traffic you want to analyze. For example, to assign the profile to an existing Ethernet interface, select **Network > Interfaces > Ethernet**, edit the interface, and select the **NetFlow Profile**. 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.
Step 3	Select **Device > Setup > Services** and define a **Service Route Configuration** for the interface that the firewall will use to send NetFlow records. You do not have to select the same interface as the one for which the firewall collects NetFlow records. You cannot select the management (MGT) interface to send NetFlow records.
Step 4	**Commit** your changes. You are now ready to monitor the firewall traffic in your NetFlow collector. Refer to your NetFlow collector documentation for instructions.



Action-Oriented Log Forwarding using HTTP

To enable better integration between your firewall and IT infrastructure, you can now trigger an action or initiate a workflow on an external HTTP-based service when a log is generated on the firewall. Forward logs from the firewall or Panorama to an HTTP(S) destination to accomplish the following tasks more easily:

- Send an HTTP-based API request directly to a third-party service to trigger an action based on the attributes in a firewall log. You can configure the firewall to work with any HTTP-based service that exposes an API, and modify the URL, HTTP header, parameters, and the payload in the HTTP request to meet your integration needs. This capability when used with the Selective Log Forwarding Based on Log Attributes allows you to forward logs that match a defined criteria so that you can automate a workflow or an action; you do not need to rely on an external system to convert syslog messages or SNMP traps to an HTTP request.

  PAN-OS 8.0, includes support for ServiceNow and VMware NSX. You can use the predefined format to send log data to ServiceNow to create an incident report and tag virtual machines using the Vmware NSX Manager. Content updates will include updates to the predefined formats added in PAN-OS 8.0 and add new predefined formats to enable integration with other third-party services.
- Tag the source or destination IP address in a log entry automatically and register the IP address and tag mapping to a User-ID agent on the firewall or Panorama, or to a remote User-ID agent so that you can respond to an event and dynamically enforce security policy. This capability extends the use for dynamic address groups that use tags as a filtering criteria to determine its members, so that you can apply security policy rules to an IP address based on tags that define its state or role on the network. For example, whenever the firewall generates a threat log, you can configure the firewall to tag the source IP address in the threat log with a specific tag name. You can then create a dynamic address group that matches on the tag name, and populates the members of the address group. And when you use this dynamic address group as a source or destination object in a policy rule, you can streamline security enforcement and limit these IP addresses from accessing network resources. Additionally, you can register the IP address and tag mappings with a User-ID agent that is configured to redistribute tags across your network infrastructure. This flow of information allows you to have better visibility, context, and control for consistently enforcing security policy irrespective of where the IP address moves across your network.

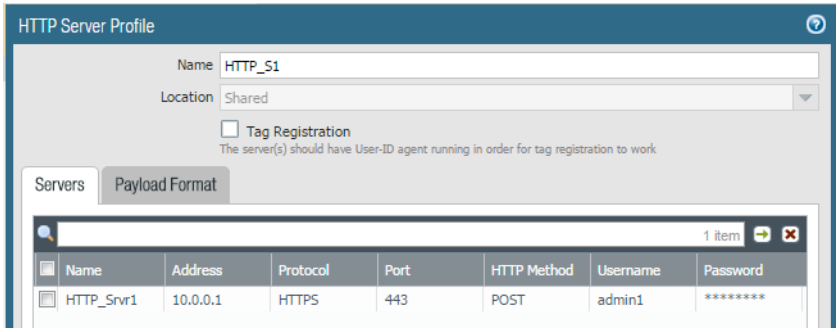
Configuration and system logs, do not support tagging because the source IP address and destination IP address attributes are not available in these log types.

Forward Logs to an HTTP Server and Enable Tagging

Step 1 Create an HTTP server profile to forward logs to an HTTP(S) destination.

The HTTP server profile allows you to specify how to access the server and define the format in which to forward logs to the HTTP(S) destination. By default, the firewall uses the management port to forward these logs.

1. Select **Device > Server Profiles > HTTP**, add a **Name** for the server profile, and select the **Location**. The profile can be **Shared** across all virtual systems or can belong to a specific virtual system.
2. Click **Add** to provide the details for each server**.** Each profile can have a maximum of 4 servers.
3. Enter a **Name** and IP **Address**.
4. Select the **Protocol** (HTTP or HTTPS). The default **Port** is 80 or 443 respectively; you can modify the port number to match the port on which your HTTP server listens.
5. Select the **HTTP Method** that the third-party service supports—PUT, POST (default), GET and DELETE.
6. Enter the **Username** and **Password** for authenticating to the server, if needed. Click **OK**.



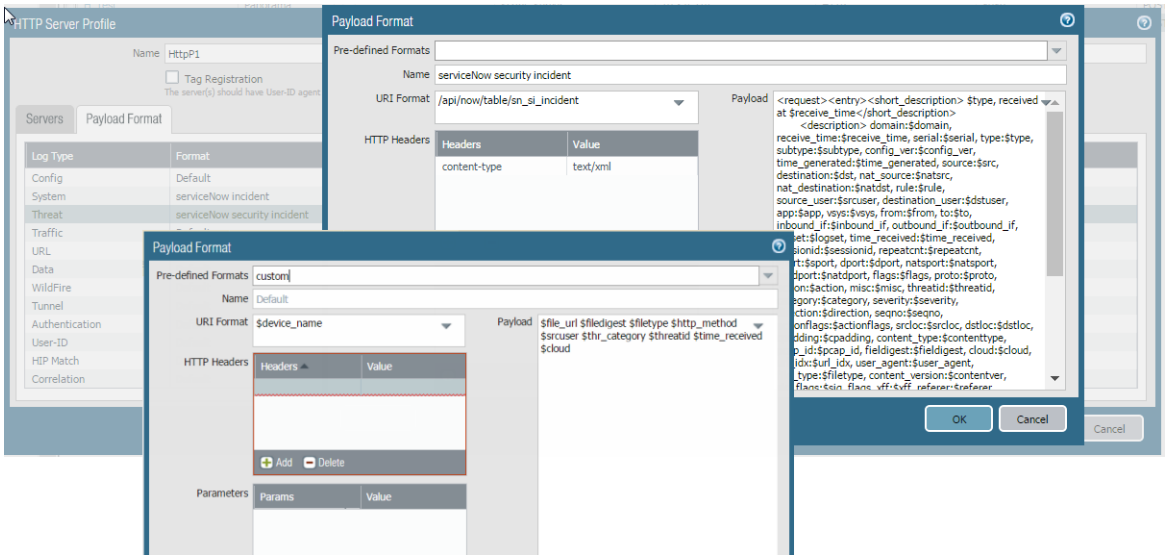
Step 2 Select **Test Server Connection** to verify network connectivity between the firewall and the HTTP(S) server.

Forward Logs to an HTTP Server and Enable Tagging (Continued)

Step 3 Configure the format for the data (*payload*) in the HTTP request.

1. Select **Payload Format**, click the **Log Type** link for each log type for which you want to define the HTTP request format. For example, select the Threat log type.
2. Select the **Pre-defined Formats** drop-down to view the formats available through content updates, or specify a custom format. Use the drop-down to select the attribute you want to include within the HTTP Header, Parameter and Value pairs, and the request payload. You can choose any attribute that selected log type supports.

   If you create a custom format, the **URI** is the resource endpoint on the HTTP service. The firewall appends the URI to the IP address you defined earlier to construct the URL for the HTTP request. Ensure that the URI and payload format matches the syntax that your third-party vendor requires.



Step 4 Trigger an action. For details, see Forward Logs to an HTTP(S) Destination.

- Define the match criteria for when the firewall will forward logs to the HTTP server, and attach the HTTP server profile to use. The match criteria allows you to specify the events (based on firewall logs) for which you want to forward logs or initiate an action on the HTTP server.
- Register or unregister a tag on a source or destination IP address in a log entry to a remote User-ID agent.

Selective Log Forwarding Based on Log Attributes

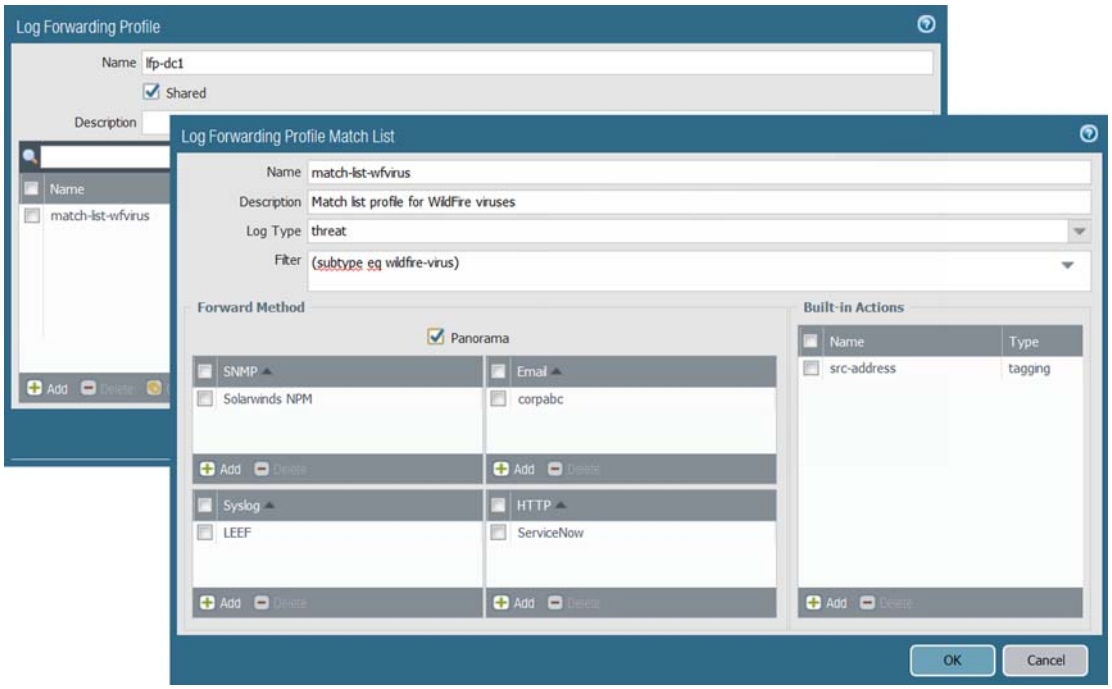
To maximize the efficiency of your incident response and monitoring operations, you can now create custom log forwarding filters based on any log attributes (such as threat type or source user). Instead of forwarding all logs or all logs of specific severity levels, you can use the filters to forward just the information you want to monitor or act on. For example, a security operations analyst who investigates malware attacks might be interested only in Threat logs with the type attribute set to wildfire-virus.

Configure Log Forwarding Based on Log Attributes	
Step 1	Configure a server profile for each external service that will receive logs from the firewall. The profiles define how the firewall connects to the services. For example, to configure an HTTP server profile, select **Device > Server Profiles > HTTP** and **Add** the profile.

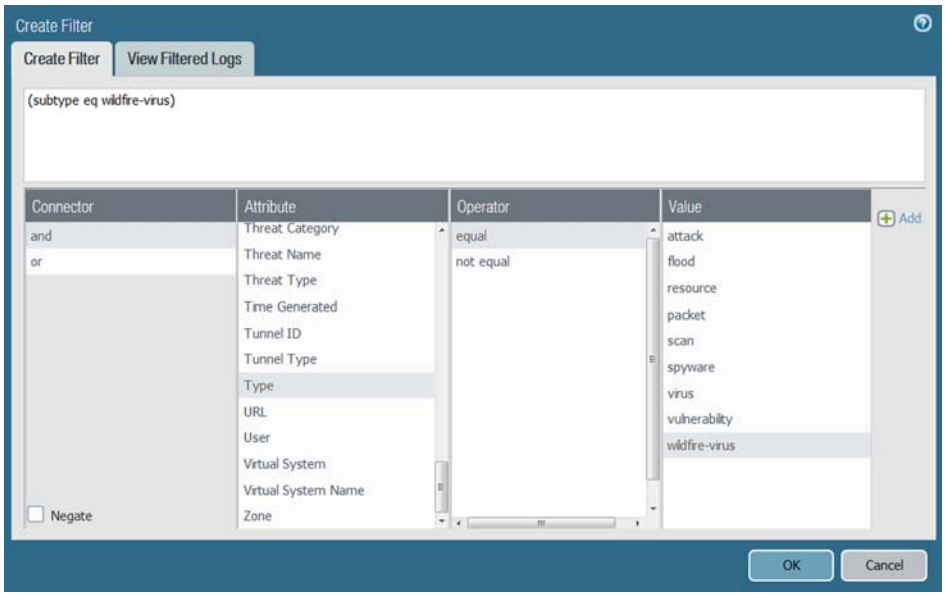
Configure Log Forwarding Based on Log Attributes

Step 2 Select **Objects > Log Forwarding** and **Add** a Log Forwarding profile to define the destinations for Traffic, Threat, WildFire Submission, URL Filtering, Data Filtering, Tunnel and Authentication logs.

In each Log Forwarding profile, **Add** one or more *match list profiles* to specify log query filters, forwarding destinations, and automatic actions such as tagging.



In each match list profile, select **Filter > Filter Builder** and **Add** filters based on log attributes.



Configure Log Forwarding Based on Log Attributes	
Step 3	Assign the Log Forwarding profile to policy rules and network zones. The firewall generates and forwards logs based on traffic that matches the rules and zones. Security, Authentication, and DoS Protection rules support log forwarding. For example, to assign the profile to a Security rule, select **Policies > Security**, edit the rule, select **Actions**, and select the **Log Forwarding** profile you created.
Step 4	Select **Device > Log Settings** and configure the destinations for System, Configuration, User-ID, HIP Match, and Correlation logs. For each log type that the firewall will forward, **Add** one or more match list profiles as you did in the Log Forwarding profile.
Step 5	**(PA-7000 Series firewalls only)** Select **Network > Interfaces > Ethernet** and **Add Interface** to configure a log card interface for log forwarding.
Step 6	**Commit** your changes.
Step 7	Verify the log destinations you configured are receiving firewall logs: • Panorama—After configuring log forwarding to Panorama, you can then verify log forwarding. • Email server—Verify that the specified recipients are receiving logs as email notifications. • Syslog server—Refer to your syslog server documentation to verify it is receiving logs as syslog messages. • SNMP trap server—Use your SNMP Manager to verify it is receiving logs as SNMP traps. • HTTP server—Verify that the HTTP destination is receiving logs.

Admin-Level Commit and Revert

You can now commit, validate, preview, save, and revert changes that you made in a Panorama or firewall configuration independent of changes that other administrators have made. This simplifies your configuration workflow because you don't have to coordinate commits with other administrators when your changes are unrelated to theirs, or worry about reverting changes other administrators made that weren't ready. When you want to activate, save, or revert some of your own changes but not others, you can also filter by configuration locations. For example, you might want to commit changes only for specific virtual systems, device group, templates, or Collector Groups.

The commit, validate, preview, save, and revert operations apply only to changes made after the last commit. To restore configurations to the state they were in before the last commit, you must load a previously backed up configuration.

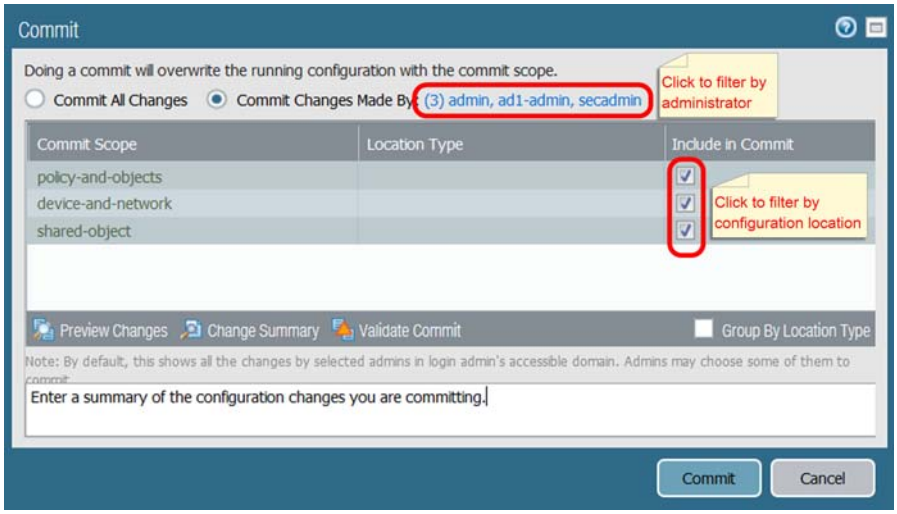
For any custom administrator role, you can enable or disable the privileges to commit, save, or revert the changes of other administrators. When configuring custom roles, note that your selections for commit privileges also apply to revert privileges.

Commit Admin-Level Changes

- Commit admin-level changes on the firewall.

  Click **Commit**, select **Commit Changes Made By**, and then filter by:
  - **Administrator**—Click the adjacent link and select the administrators. This option is available only if your administrative role has the privilege to commit the changes of other administrators. Otherwise, you can commit only your own changes.
  - **Configuration location**—In the Commit Scope, clear the check boxes for any changes that are not ready to activate.

  After you finish filtering, **Commit** the selected changes.



Commit Admin-Level Changes (Continued)

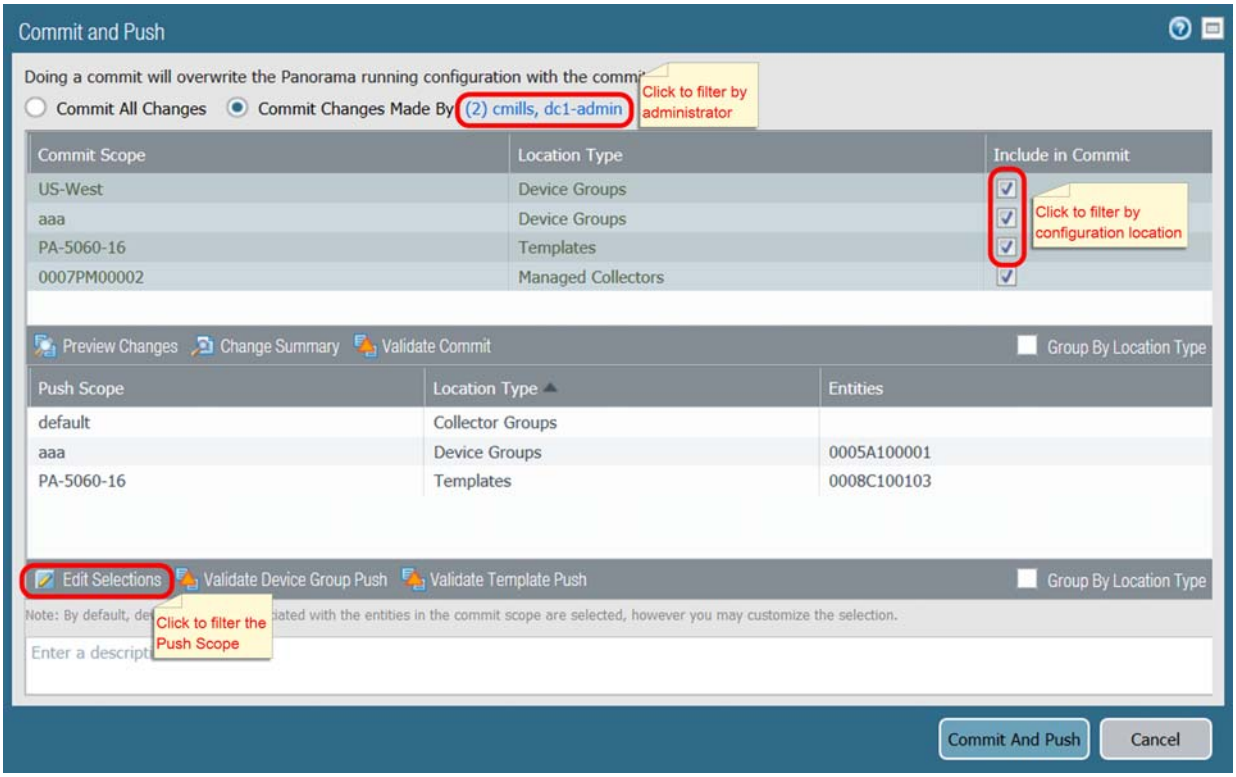
- Commit admin-level changes on Panorama and push the changes to managed firewalls and Log Collectors as part of the same operation.

  Select **Commit > Commit and Push**, select **Commit Changes Made By**, and then filter by:

  - **Administrator**—Click the adjacent link and select the administrators. This option is available only if your administrative role has the privilege to commit the changes of other administrators. Otherwise, you can commit only your own changes.
  - **Configuration location**—In the Commit Scope, clear the check boxes for any changes that are not ready to activate.

  By default, the Push Scope includes all the device groups, templates, and Collector Groups that have configuration changes. However, you can **Edit Selections** to filter what the push operation will include.

  After filtering the Commit Scope and Push Scope, **Commit and Push** the selected changes.

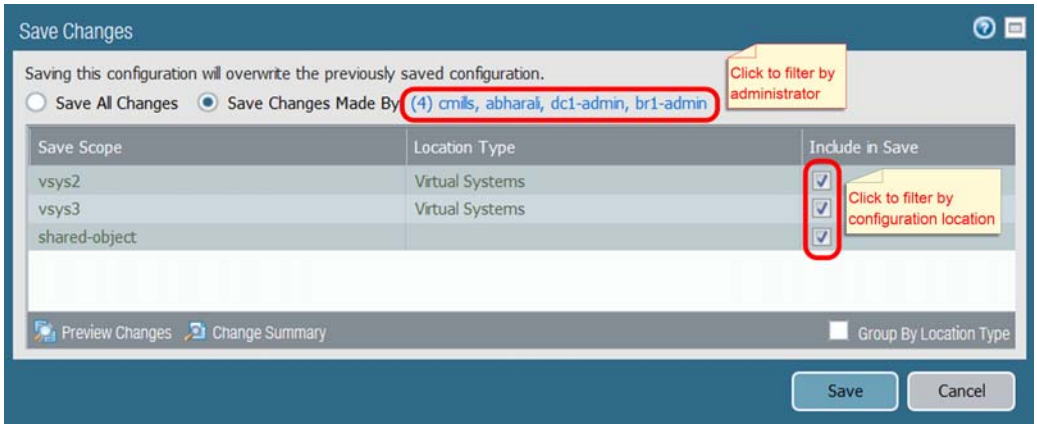


To commit changes on Panorama that are not ready to activate on firewalls and Log Collectors, select **Commit > Commit to Panorama**. When the changes are ready to activate, you can then select **Commit > Push to Devices**. When pushing configurations to managed devices, Panorama 8.0 pushes the running configuration, which is the configuration that is committed to Panorama. Therefore, you must commit changes to Panorama before pushing those changes to managed devices.

Commit Admin-Level Changes (Continued)

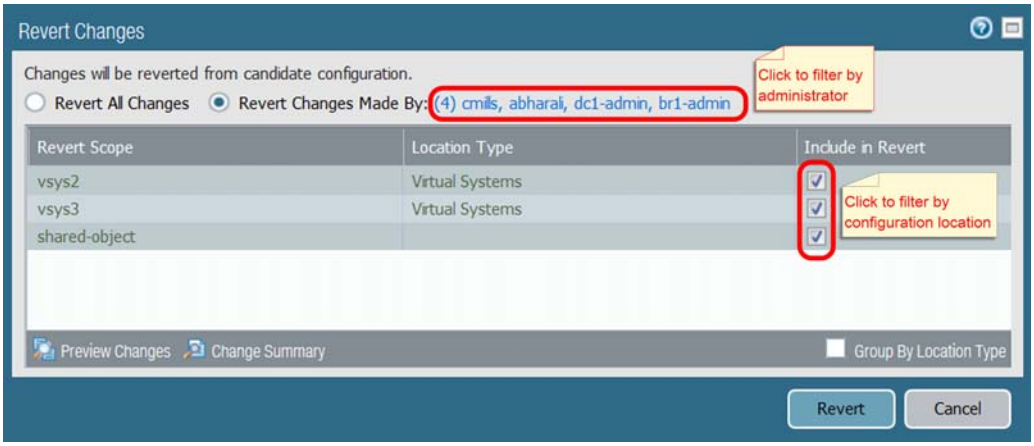
- Save admin-level changes on the firewall or Panorama.
  Select **Config > Save Changes**, select **Save Changes Made By**, and then filter by:
  - **Administrator**—Click the adjacent link and select the administrators. This option is available only if your administrative role has the privilege to save the changes of other administrators. Otherwise, you can save only your own changes.
  - **Configuration location**—In the Save Scope, clear the check boxes for any changes that are not ready to save.

  After you finish filtering, **Save** the selected changes.



- Revert admin-level changes on the firewall or Panorama.
  Select **Config > Revert Changes**, select **Revert Changes Made By**, and then filter by:
  - **Administrator**—Click the adjacent link and select the administrators. This option is available only if your administrative role has the privilege to commit and revert the changes of other administrators. Otherwise, you can revert only your own changes.
  - **Configuration location**—In the Revert Scope, clear the check boxes for any changes you do not want to revert.

  After you finish filtering, **Revert** the selected changes.



Extended SNMP Support

PAN-OS support for Simple Network Management Protocol (SNMP) now includes the following features. To access the latest MIBs, refer to SNMP MIB Files.

Feature	Description
SNMP Monitoring of Logging Statistics	You can now monitor a broader range of logging statistics, including logging rate, disk usage, retention periods, the forwarding status from individual firewalls to Panorama and external servers, and the status of firewall-to-Log Collector connections. Monitor logging statistics to plan improvements to your log collection architecture, evaluate the health of firewall and Panorama logging functions, and troubleshoot issues such as dropped logs. The following MIBs enable monitoring for logging statistics: • The new panDeviceLogging MIB displays logging statistics for each firewall. • New objects in the panLogCollector MIB display logging statistics for each Log Collector.
SNMP Monitoring of Dedicated HA2 Interfaces	For firewalls deployed in a high availability (HA) configuration, you can now monitor the dedicated HA2 interfaces of firewalls, in addition to the HA1, HA2 backup, and HA3 interfaces. To see SNMP statistics for dedicated HA2 interfaces, use the IF-MIB and interfaces MIB.
Hardware IP Address Blocking	To see the counts of source IP addresses blocked by hardware and software, the firewall supports one updated global counter and two new global counters in the panGlobalCounters MIB: • `flow_dos_blk_num_entries` shows the total sum of IP address entries on the hardware block table and Block IP list (blocked by hardware and software). • `flow_dos_blk_hw_entries` shows the count of IP address entries on the hardware block table that were blocked by hardware. • `flow_dos_blk_sw_entries` shows the count of IP addresses entries on the Block IP list that were blocked by software. You can view the counters using the CLI, for example: `> show counter global name flow_dos_blk_num_entries`
Packet Buffer Protection	This release introduces new MIBs to track the active connections per second (CPS) for virtual system (VSYS), zone, and interface. Use this information as a guide to help better configure Zone and DoS protection profiles. Each set of MIBs display the active CPS for TCP, UDP, and Other IP connections. • VSYS—`panVsysEntry`, `panVsysActiveTcpCps`, `panVsysActiveUdpCps`, `panVsysActiveOtherIpCps` • Zone—`panZoneEntry`, `panZoneActiveTcpCps`, `panZoneActiveUdpCps`, `panZoneActiveOtherIpCps` • Interface—`panIfEntry`, `panIfActiveTcpCps`, `panIfActiveUdpCps`, `panIfActiveOtherIpCps`

Panorama Features

Traps Log Ingestion on Panorama

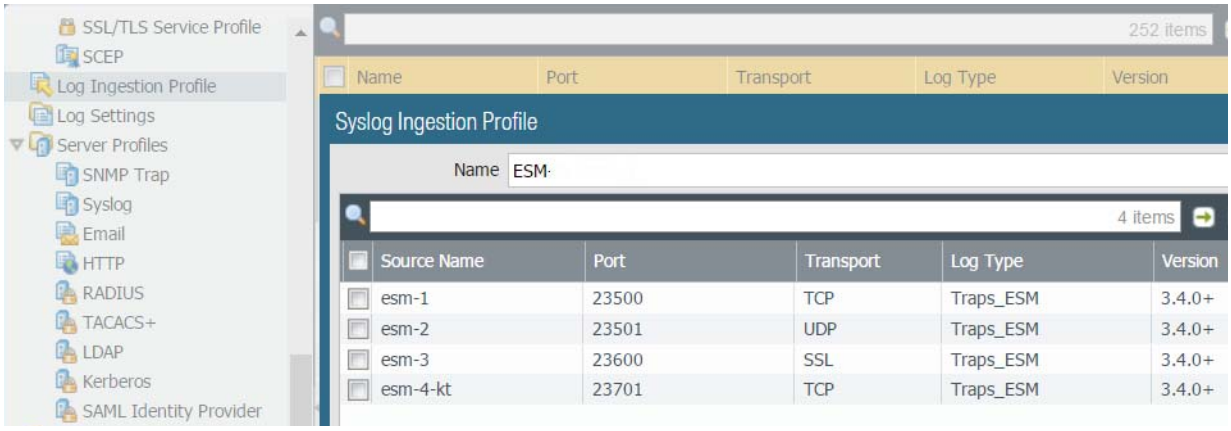
Panorama can now serve as a Syslog receiver that can ingest logs from the Traps ESM components using Syslog over TCP, UDP, or SSL. When you forward security events that the Traps agents report to the ESM Server on to Panorama, Panorama correlates discrete security events that occur on the endpoints with what's happening on the network to trace any suspicious or malicious activity across the endpoints and the firewalls. This integrated view gives you more context on the chronology of events and the evidence you need to detect, identify, and respond to an incident.

Panorama virtual appliance in legacy mode cannot ingest Traps logs.

Configure Panorama to Receive Traps Logs

Step 1 Define the log ingestion profile on Panorama.

1. Select **Panorama > Log Ingestion Profile**, and click **Add**.
2. Enter a **Name** for the profile.
3. Click **Add** and enter the details for the ESM Server. You can add up to four ESM Servers to a profile.
4. Enter a **Source Name**.
5. Specify the **Port** on which Panorama will be listening for syslog messages. The range is 23000 to 23999.
6. Select the **Transport** layer protocol—TCP, UDP, or SSL.
7. Select Traps_ESM for **External Log type** and 3.4.0+ from the **Version** drop-down.
   As Traps log formats are updated, the updated log definitions will be available through content updates on Panorama.

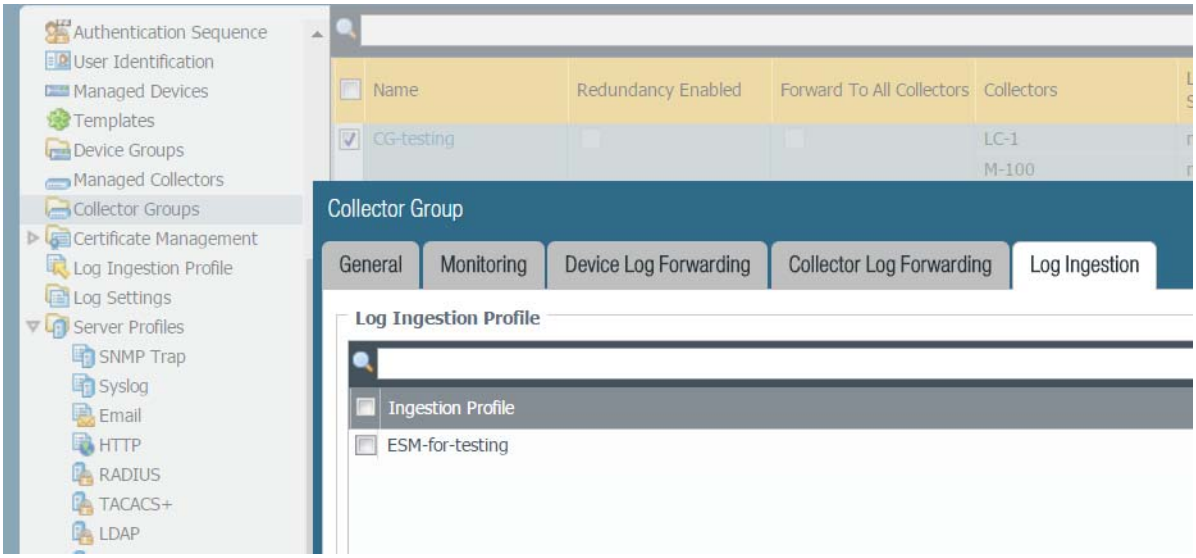


Configure Panorama to Receive Traps Logs (Continued)

Step 2 Attach the log ingestion profile to a Collector Group.

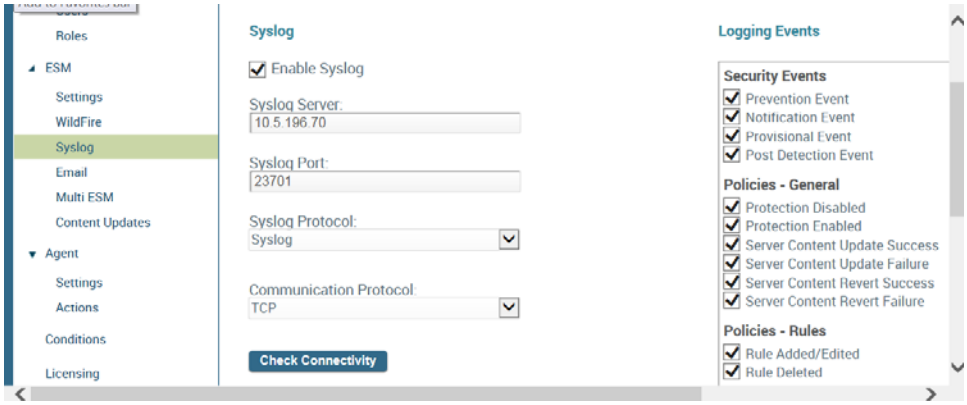
1. Select **Panorama > Collector Groups > Log Ingestion** and **Add** the log ingestion profile so that the Collector Group can receive logs from the ESM Server(s) listed in the profile.

   If you are enabling SSL for secure syslog communication between Panorama and the ESM Server(s), you must attach an certificate for secure Syslog communication between the ESM Servers and the Managed Collectors in the Collector Group. In **Panorama > Managed Collectors > General**, select the certificate to use for **Inbound Certificate for Secure Syslog**).



2. **Commit** changes to Panorama and the Collector Group.

Step 3 Configure Panorama as a Syslog receiver on the ESM Server. Enter the **Syslog Port** you specified in the log ingestion profile on Panorama.

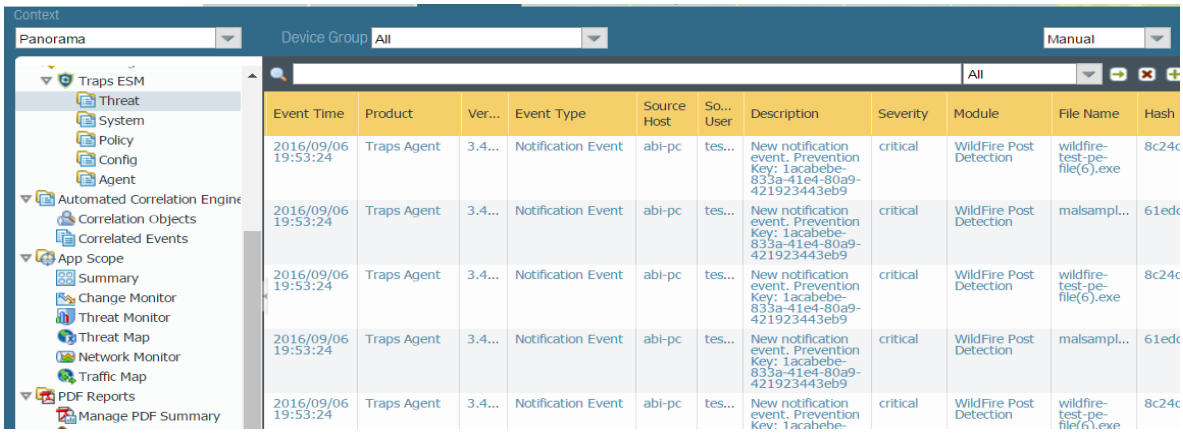


For details on the other forwarding settings, refer to the Traps 3.4 Administrator's Guide.

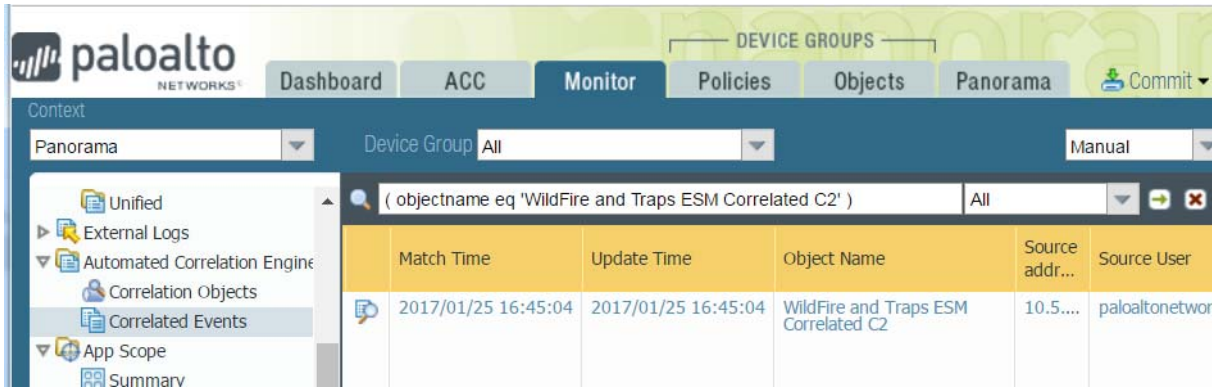
Configure Panorama to Receive Traps Logs (Continued)

Step 4 View ESM logs and correlated events on Panorama.

1. Select **Monitor > External Logs > Traps ESM** to view the logs ingested in to Panorama.



2. Select **Monitor > Automated Correlation Engine > Correlated Events** to view correlated events that Panorama generates when a Traps agent and the firewall have observed command and control activity from one or more infected hosts on your network.



Extended Support for Multiple Panorama Interfaces

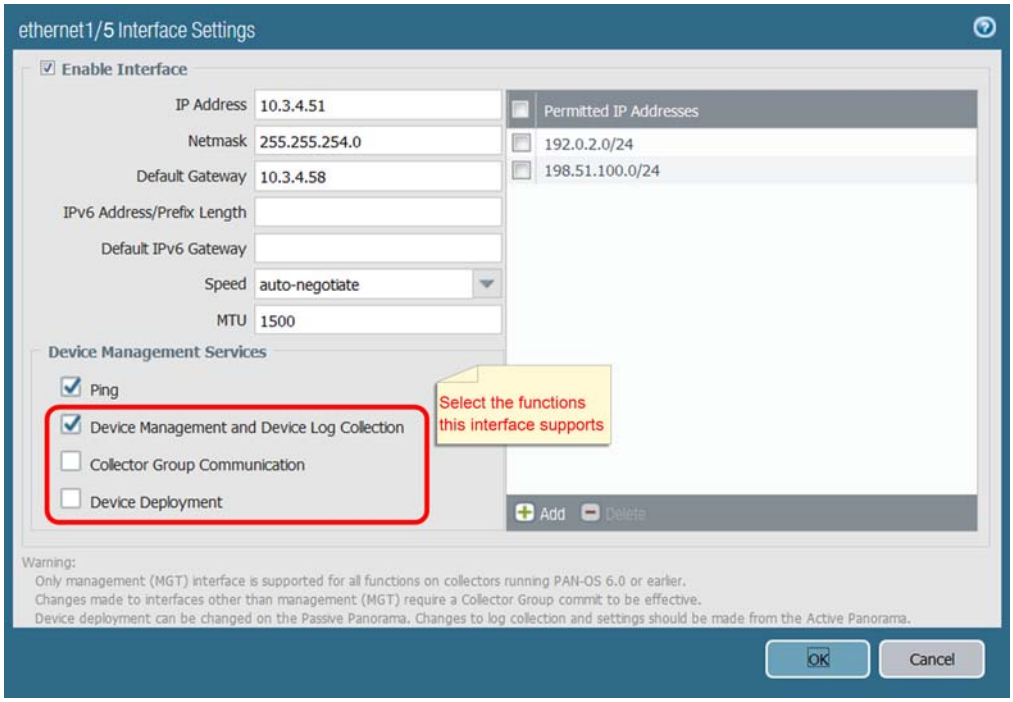
To accommodate network segmentation and security requirements in a large-scale deployment, you can now separate the Panorama management functions from the device management and log collection functions by assigning them to separate interfaces on the M-500 and M-100 appliances. To minimize bandwidth competition that can impede the performance of Panorama, you can implement load balancing for device management and log collection by using multiple interfaces for those functions. You can further reduce the traffic load on the management (MGT) interface by selecting some other interface for deploying software and content updates to firewalls and Log Collectors. Additional interfaces on the M-100 appliance (Ethernet3) and M-500 appliance (Ethernet3, Ethernet4, and Ethernet5) are available to support multiple interfaces.

Perform the following steps to configure multiple interfaces on a high availability (HA) pair of Panorama management servers and on Dedicated Log Collectors.

Configure Panorama and Dedicated Log Collectors to Use Multiple Interfaces

Step 1 Configure the interfaces on the active Panorama management server—Select **Panorama > Setup > Interfaces** and edit each interface.

In an environment with high logging rates, you can assign the **Device Management and Device Log Collection** function to the Ethernet4 and Ethernet5 interfaces on the M-500 appliance for 10Gbps throughput. The other interfaces on the M-500 and M-100 appliances support only 1Gbps.



Configure Panorama and Dedicated Log Collectors to Use Multiple Interfaces (Continued)	
Step 2	Configure each Log Collector to connect with a Panorama interface that has **Device Management and Device Log Collection** enabled—On the active Panorama, select **Panorama > Managed Collectors**, edit the Log Collector, and enter the IP addresses of interfaces on the: • Active Panorama (**Panorama Server IP**) • Passive Panorama (**Panorama Server IP 2**)  To support a segmented network, you can connect the Log Collectors in each subnetwork to separate Panorama interfaces on each HA peer.

Step 3	Enable connectivity between the Panorama management servers and Log Collectors—Access each Log Collector CLI and run the following commands, where `<IPaddress1>` is for the active Panorama and `<IPaddress2>` is for the passive Panorama. The IP addresses must be the same as those you configured in the previous step.
	`> configure`
	`# set deviceconfig system panorama-server <IPaddress1> panorama-server-2 <IPaddress2>`
	`# commit`

Step 4	Configure an interface on the passive Panorama management server to deploy updates in case the active Panorama fails over—On the passive Panorama, select **Panorama > Setup > Interfaces**, edit the interface, and select **Device Deployment**.
Step 5	Configure the interfaces that the Log Collectors will use to collect logs from firewalls and communicate with other Log Collectors—On the active Panorama, select **Panorama > Managed Collectors**, edit the Log Collector, assign the **Device Log Collection** function to one or more interfaces, and assign the **Collector Group Communication** function to one interface.  In an environment with high logging rates, you can assign the **Device Log Collection** function to the Ethernet4 and Ethernet5 interfaces on the M-500 appliance for 10Gbps throughput.
Step 6	On the active Panorama, select **Commit > Commit and Push** to activate your changes on Panorama and push the changes to Collector Groups.
Step 7	Configure each firewall to connect with a Panorama interface that has **Device Management and Device Log Collection** enabled—On the active Panorama, select **Device > Setup > Management**, select the **Template** that the firewalls are assigned to, edit the Panorama Settings, and enter the IP addresses of interfaces on the: • Active Panorama (first **Panorama Servers** field) • Passive Panorama (second **Panorama Servers** field)  To support a segmented network, you can connect the firewalls in each subnetwork to separate Panorama interfaces on each HA peer.
Step 8	On the active Panorama, select **Commit > Commit and Push** to activate your changes on Panorama and push the template changes to firewalls.

Streamlined Deployment of Software and Content Updates from Panorama

Instead of pushing software and content updates to one firewall or Log Collector at a time, Panorama now notifies the devices when updates are available and the devices then retrieve the updates in parallel. This enables Panorama to deploy software and content updates to managed devices more quickly. The procedures to deploy updates have not changed (see Upgrade Firewalls Using Panorama and Deploy an Update to Log Collectors) but you must leave port 28443 open on Panorama for firewalls and Log Collectors to retrieve the updates. Only firewalls that run PAN-OS 8.0 and Log Collectors that run Panorama 8.0 will retrieve updates; for devices running earlier releases, Panorama still pushes the entire update package instead of sending notifications.

If you want to reserve the management (MGT) interface for management traffic and log collection, you can use a separate interface for the traffic associated with deploying updates (see Extended Support for Multiple Panorama Interfaces).

Logging Enhancements on the Panorama Virtual Appliance

You can now create a Log Collector that runs locally on the Panorama virtual appliance. Because the local Log Collector supports multiple virtual logging disks, you can increase log storage as needed while preserving existing logs. The local Log Collector supports up to 12 virtual disks for 24TB of log storage on a single Panorama virtual appliance and up to 48TB on a high availability (HA) pair. Without a local Log Collector, Panorama supports only one logging disk with up to 8TB of storage.

You cannot deploy the Panorama virtual appliance as a Dedicated Log Collector.

The virtual appliance supports NFS log storage only in Legacy mode, not in Panorama mode. After switching to Panorama mode, you must migrate the logs that are in the NFS storage to the virtual disks on the local Log Collector.

After you upgrade to Panorama 8.0, the Panorama virtual appliance will be in Legacy mode by default. To enable support for a local Log Collector, you must first increase resources on the appliance and switch it to Panorama mode. The minimum resources include a larger system disk (81GB), more CPUs and memory based on the log storage capacity, and an additional virtual logging disk that has at least as much capacity as is used for logs in Legacy mode.

If Panorama is deployed in an high availability (HA) configuration, perform the following steps on the secondary peer first and then on the primary peer.

Configure a Log Collector on the Panorama Virtual Appliance	
Step 1	Determine which system resources you need to increase by accessing the Panorama CLI and running the following command: `> request system system-mode panorama`
Step 2	Use your VMware ESXi vSphere Client to increase the memory and CPUs and to add a new system disk.
Step 3	Use the Panorama CLI to copy the data from the original system disk to the new system disk: `> request system clone-system-disk target sdb`
Step 4	Use the vSphere Client to remove the old system disk and add a virtual logging disk.
Step 5	Use the Panorama CLI to switch from Legacy mode to Panorama mode. `> request system system-mode panorama`
Step 6	**(HA only)** Repeat Step 1 through Step 5 on the primary Panorama to switch it to Panorama mode. This step triggers failover. After switching the mode, restore the primary Panorama to the active HA state and ensure both HA peers are functional.
Step 7	Use the Panorama CLI to migrate existing logs to the new virtual logging disk. In an HA configuration, perform this only on the primary Panorama. `> request logdb migrate vm start`
Step 8	To verify that the existing logs are available, log in to the Panorama web interface, select **Panorama > Monitor**, select a log type that you know matches some existing logs (for example, **Panorama > Monitor > System**), and verify that the logs display.

Content Inspection Features

Credential Phishing Prevention

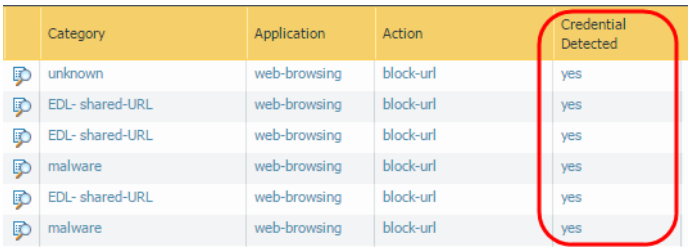
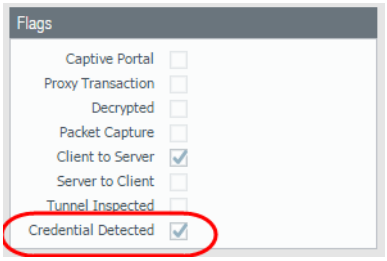
Phishing sites are sites that attackers disguise as legitimate websites with the aim to steal user information, especially the user credentials that provide access to your network. When a phishing email enters a network, it takes just a single user to click the link and enter credentials to set a breach in motion. You can now identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site's URL category. This allows you to block users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and sanctioned sites.

Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials. You can choose what websites you want to either allow, alert on, or block corporate credential submissions to based on the URL category of the website. Alternatively, you can present a page that warns users against submitting credentials to sites classified in certain URL categories. This gives you the opportunity to educate users against reusing corporate credentials, even on legitimate, non-phishing sites. In the event that corporate credentials are compromised, this feature allows you to identify the user who submitted credentials so that you can remediate.

Take the following steps to prevent phishing attempts by controlling the sites to which your users can submit credentials.

Enable Credential Phishing Prevention		
Step 1	Decide what user credential detection method you want the firewall to use to detect corporate credential submissions and configure User-ID as required to support the selected method.	Each of the Methods to Check for Corporate Credential Submissions requires a different User-ID configuration to check for corporate credential submissions: • If you plan to use the group mapping method, which detects whether a user is submitting a valid corporate username, Map Users to Groups. • If you plan to use the IP user mapping method, which detects whether a user is submitting a valid corporate username that matches the username of the user logged into the source IP address of the session, Map IP Addresses to Users. • If you plan to use the domain credential filter method, which detects whether a user is submitting a valid username and password and that those credentials match the user who is logged in to the source IP address of the session, Configure Credential Detection with the Windows-based User-ID Agent and Map IP Addresses to Users.

Enable Credential Phishing Prevention		
Step 2	Configure URL Filtering to detect corporate credential submissions to websites that are in allowed URL categories.  If you have not done so already, configure a best practice URL Filtering profile to ensure protection against URLs that have been observed hosting malware or exploitive content.	1. Select **Objects > Security Profiles > URL Filtering** and **Add** or modify a URL Filtering profile. 2. On the **User Credential Detection** tab, select one of the Methods to Check for Corporate Credential Submissions: • **Use IP User Mapping—**Checks if username submissions match the user logged into the source IP address of the session. • **Use Domain Credential Filter**—Checks for valid corporate usernames and password submissions and verifies that the submitted credentials match the user logged into the source IP address of the session. • **Use Group Mapping**—Checks that submitted usernames match a username in the user-to-group mapping table. With group mapping, you can apply credential detection to **any** part of the directory, or limit it to selected groups that have access to your most sensitive resources, such as IT. 3. Set the **Valid Username Detected Log Severity** the firewall uses to log detection of corporate credential submissions. By default, the firewall logs these events as medium severity.
Step 3	Block (or alert) on credential submissions to allowed sites.  The firewall automatically skips checking credential submissions on sites that have never been observed hosting malware or phishing attacks to ensure the best performance even if you enable checks in the corresponding category. The list of sites on which the firewall will skip credential checking is automatically updated via Application and Threat content updates.	1. On the **Categories** tab, for each Category to which **Site Access** is allowed, select how you want to treat **User Credential Submissions**: • **alert**—Allow users to submit credentials to the website, but generate a URL Filtering log each time a user submits credentials to sites in this URL category. • **allow**—(default) Allow users to submit credentials to the website. • **block**—Block users from submitting credentials to the website and display a response page. • **continue**—Present a response page to users that requires them to click Continue to continue with credential submission. 2. Select **OK** to save the URL Filtering profile.
Step 4	Apply the updated URL filtering and credential detection settings to the Security policy rules that allow web traffic.	1. Select **Policies > Security** and **Add** or modify a Security policy rule. 2. Select **Actions** and set the **Profile Type** to **Profiles**. 3. Select the new or updated **URL Filtering** profile to attach it to the Security policy rule. 4. Select **OK** to save the Security policy rule.
Step 5	**Commit** the URL Filtering profile and Security policy rule updates.	

Enable Credential Phishing Prevention	
Step 6 Monitor credential submissions the firewall detects. A new ACC widget provides a view into the number of users who have visited malware and phishing sites. Select **ACC > Hosts Visiting Malicious URLs**.	Select **Monitor > Logs > URL Filtering**. The new **Credential Detected** column indicates events where the firewall detected a HTTP post request that included a valid credential:  (To display this column, hover over any column header and click the arrow to select the columns you'd like to display). Log entry details also indicate credential submissions: 

	Category	Application	Action	Credential Detected
	unknown	web-browsing	block-url	yes
	EDL- shared-URL	web-browsing	block-url	yes
	EDL- shared-URL	web-browsing	block-url	yes
	malware	web-browsing	block-url	yes
	EDL- shared-URL	web-browsing	block-url	yes
	malware	web-browsing	block-url	yes

Telemetry and Threat Intelligence Sharing

You can now participate in telemetry, a community-driven approach to threat prevention. Telemetry allows the firewall to periodically collect and share information about applications, threats, and device health with Palo Alto Networks. Sharing threat intelligence provides the following benefits:

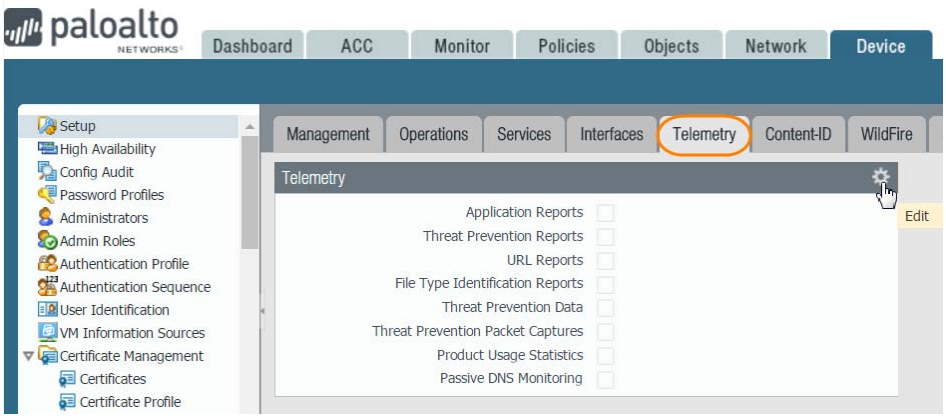
- Enhanced intrusion prevention system (IPS) and spyware signatures delivered to you and other customers worldwide. For example, when a threat event triggers vulnerability or spyware signatures, the firewall shares the URLs associated with the threat with the Palo Alto Networks threat research team, so they can properly classify the URLs as malicious.
- Rapid testing and evaluation of experimental threat signatures with no impact to your network, so that critical threat prevention signatures can be released to all customers faster.
- Improved accuracy and malware detection abilities within PAN-DB URL filtering, DNS-based command-and-control (C2) signatures, and WildFire.

You can choose which telemetry data to share with Palo Alto Networks. The firewall collects the data from your firewall logs; the combination of log types and log data depend on the Telemetry settings you enable.

An enhancement of the Statistics Service feature in firewalls running PAN-OS 7.1 and earlier, telemetry is an opt-in feature. Palo Alto Networks does not share your telemetry data with other customers or third-party organizations.

Enable Threat Intelligence Sharing

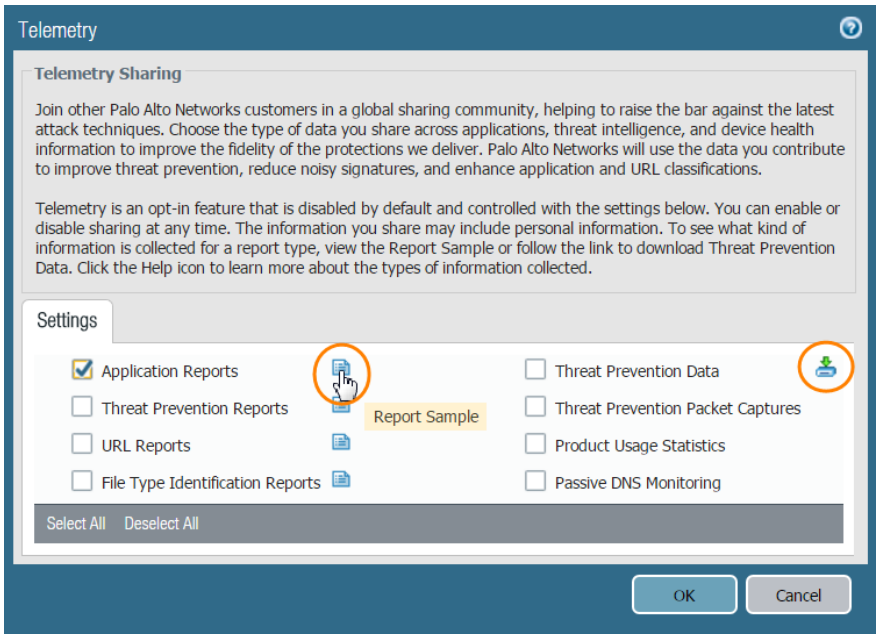
Step 1 Select **Device > Setup > Telemetry**, and edit the Telemetry settings.



Step 2 Select the telemetry data you want to share with Palo Alto Networks. For more specific descriptions of this data, see What Telemetry Data Does the Firewall Collect?

If you have previously configured your firewall to share data through the Statistics Service (PAN-OS 7.1), the Telemetry settings that match the Statistics Service settings are selected and enabled by default.

Step 3 View the telemetry data (or examples of the data) that the firewall collects. See Enable Threat Intelligence Sharing.



Step 4 Click **OK** and **Commit** your changes.

Palo Alto Networks Malicious IP Address Feeds

With an active Threat Prevention subscription, Palo Alto Networks now provides two malicious IP address feeds. These IP address feeds allow you to leverage the latest Palo Alto Networks threat intelligence when blocking traffic by IP address.

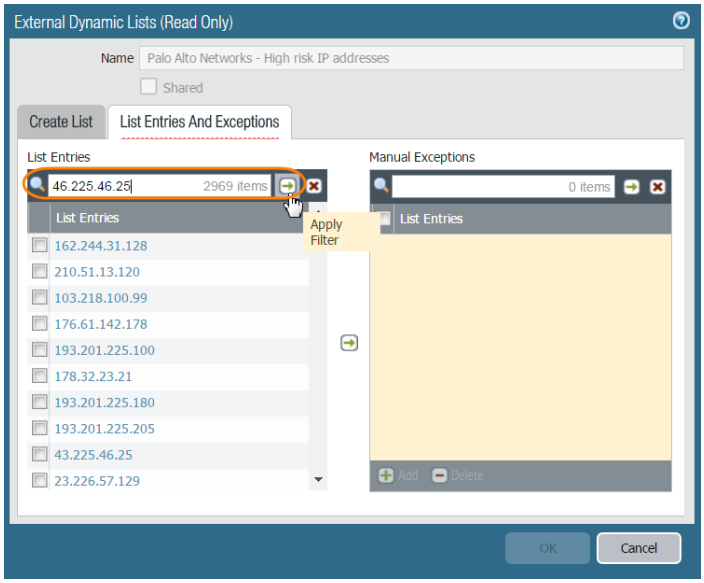
- **Palo Alto Networks - Known malicious IP addresses**—Contains IP addresses that Palo Alto Networks has verified as malicious.
- **Palo Alto Networks - High risk IP addresses**—Contains malicious IP addresses from threat advisories issued by trusted third-party organizations.

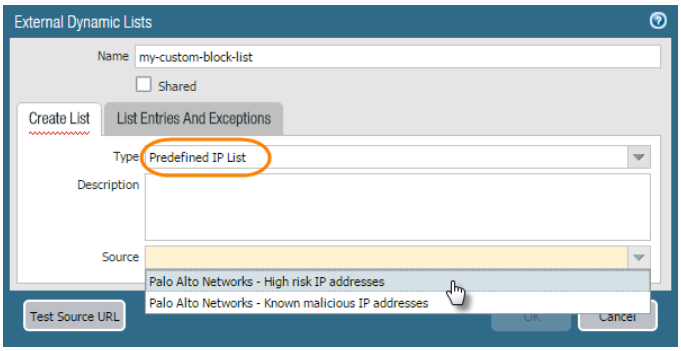
Palo Alto Networks delivers updated versions of the IP address feeds as part of the daily antivirus content updates for the firewall. Entries from the most recent versions of the feeds replace the entries from older versions. The feeds are *predefined*, which means that you cannot modify their contents. However, you can create a new external dynamic list that uses either of the predefined IP address feeds as a source. This gives you the flexibility of excluding IP addresses from the feed, if necessary.

Assess your organization's threat prevention strategy when referencing the Palo Alto Networks malicious and high-risk IP address feeds in security policy rules. Palo Alto Networks employs a variety of safety checks to prevent shared or legitimate IP addresses from being added to the known malicious IP address feed; however, it's possible for an IP address in the feed to be mapped to multiple servers, some of which might not cause malicious behavior. Furthermore, while the high risk IP address feed comes from trusted third-party sources, Palo Alto Networks does not regulate the contents of this feed.

To monitor traffic associated with the known malicious or high-risk IP address feed, create a security policy rule reserved for blocking traffic from the feed, then filter the Traffic log by the rule you created.

Use a Palo Alto Networks Malicious IP Address Feed in Policy		
Step 1	Confirm that the firewall can access the Palo Alto Networks malicious IP address feeds.	• Confirm that you have activated your Threat Prevention subscription on the firewall. Select **Device > Licenses** to check that your subscription is valid. • Confirm that you have downloaded and installed the latest Antivirus version on your firewall.

Use a Palo Alto Networks Malicious IP Address Feed in Policy (Continued)	
Step 2 View the contents of the Palo Alto Networks malicious IP address feeds directly on the firewall.	View external dynamic list entries for the following malicious IP address feeds: • **Palo Alto Networks - High risk IP addresses** • **Palo Alto Networks - Known malicious IP addresses** Filter the list to check that it does not contain IP addresses you need to access.  If you have an active AutoFocus subscription, hover over any of the IP addresses in the list to open the drop-down and view an AutoFocus Intelligence Summary for it. You cannot delete, clone, edit, or exclude IP addresses from a Palo Alto Networks malicious IP address feed.

Use a Palo Alto Networks Malicious IP Address Feed in Policy (Continued)	
Step 3 (Optional) Create a new external dynamic list that uses a Palo Alto Networks IP address feed as a source.	• In the Type drop-down, select **Predefined IP List**. • Select a Palo Alto Networks IP address feed to use as a **Source** for your external dynamic list.  • (Optional) Exclude entries from the external dynamic list (new in PAN-OS 8.0). The firewall updates the custom external dynamic list you just created each time it receives an update for the Palo Alto Networks IP address feed, but your list exceptions are preserved.
Step 4 Use a Palo Alto Networks malicious IP address feed to block network traffic.	Enforce policy on entries in an external dynamic list. Use the known malicious or high-risk IP address feed (or custom list based on either of these feeds) as a source or destination address object in a Security policy rule.

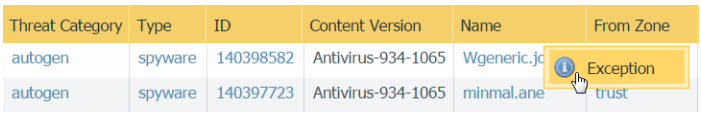
Enhanced Coverage for Command and Control (C2) Traffic

Command-and-control (C2) describes when a compromised system is surreptitiously communicating with an attacker's remote server to receive malicious commands or exfiltrate data. A new type of signature that detects C2 traffic is now generated automatically. While C2 protection is not new, previous signatures looked for an exact match to domain names in DNS queries or full URLs in HTTP client requests to identify a C2 host. The new, automatically-generated C2 signatures detect certain patterns in C2 traffic instead of the C2 host. This enables the firewall to provide more accurate, timely, and robust C2 detection even when the C2 host is unknown or changes rapidly.

To benefit from the enhanced C2 protection, you'll need a Threat Prevention license—the new, automated C2 signatures are made available with hourly Antivirus updates, and further C2 protection continues to be delivered with the Applications and Threats updates. Additionally, both the Palo Alto Networks Threat Vault and AutoFocus are integrated with the firewall, and you can leverage these resources to immediately access more information about C2 attacks the firewall detects.

Enable C2 Protection and Learn More About C2 Attacks		
Step 1	Select **Device > Licenses** and confirm that the firewall Threat Prevention license is active.	
Step 2	Select **Device > Dynamic Updates** and enable the firewall to get the latest Antivirus updates every hour. The extended, automated C2 protection this feature introduces is made available with the latest Antivirus updates; however, Applications and Threats content updates also continue to provide C2 protection. To enable full coverage for C2 attacks, make sure that you also enable the firewall to check for the latest Applications and Threats content every 30 minutes (see New Scheduling Options for Application and Threat Content Updates).	
Step 3	Enable the firewall to block C2 activity it detects.	1. Select **Objects > Security Profiles > Antivirus** and **Add** or modify an Antivirus profile. The default action for C2 signatures is **Reset Client**; this means that when the firewall detects C2 communication, it resets the client-side TCP connection or drops the UDP connection. Setting up an Antivirus profile defines how you want the firewall to treat C2 attacks that match the new automated C2 signatures—also set up an Anti-Spyware profile to make sure that the firewall is blocking all C2 attacks. 2. Attach the Antivirus profile (and Anti-Spyware profile) to a security policy rule: a. Select **Policies > Security** and **Add** or modify a security policy rule. b. Select **Actions** and in the Profile Settings, set the Profile Type to **Profiles**. c. Select the Anti-Spyware profile you want to apply to traffic matched to this rule. d. Click **OK**.

Enable C2 Protection and Learn More About C2 Attacks (Continued)	

Step 4 Find out more about C2 activity the firewall detects.	• Monitor C2 activity:
	Select **Monitor > Logs > Threat**. Events the firewall detected based on the automatically-generated spyware signatures are logged with the **Threat Category** autogen and the **Type** spyware. Add the following filter to show only log entries for these events:`(subtype eq spyware) and (category-of-threatid eq autogen)`.
	• Find out more about a specific C2 event:
	  • Select the spyglass icon to view in-depth details for the logged event.
	  • (New) Hover over a threat **Name** and click **Exception** to learn more about the type of threat detected and to see if the signature that detected the threat is configured as an exception to certain security policy rules.
	 
	
	TLearn more about how you can use Globally Unique Threat IDs to gain context for a threat signature or create a threat exception.
	  • Hover over an IP address, URL, or domain to search for that artifact in AutoFocus—AutoFocus can reveal if the artifact is frequently found with malware, if it is associated with malware variants, and whether the artifact is targeted or pervasive throughout your network, industry, or globally. This feature requires an AutoFocus license.

Data Filtering Support for Data Loss Prevention (DLP) Solutions

Data filtering is enhanced to work with third-party, endpoint DLP solutions that populate file properties to indicate sensitive content, enabling the firewall to enforce your DLP policy. To better secure this confidential data, you can now enable data filtering to identify the file properties and values set by a DLP solution and then log or block the files the data filtering profile identifies.

While this feature is supported in previous release versions, it required you to use regular expression to define the data patterns on which you want the firewall to filter. This data filtering enhancement introduces a more simplified and intuitive workflow to prevent confidential information from leaving your network, including:

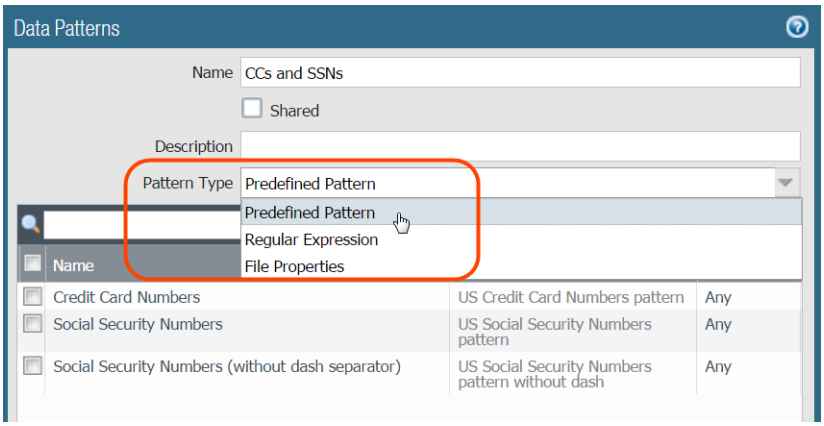
- Built-in settings allow you to easily enable the firewall to scan for file properties and specific, associated values. If you're using a DLP solution, you can populate these settings based on your DLP policy.
- New predefined data patterns enable you to quickly set up social security and credit card number detection.

Data pattern objects previously defined to filter for credit card numbers, social security numbers, and regular expression patterns will look a little different after the upgrade to PAN-OS 8.0.

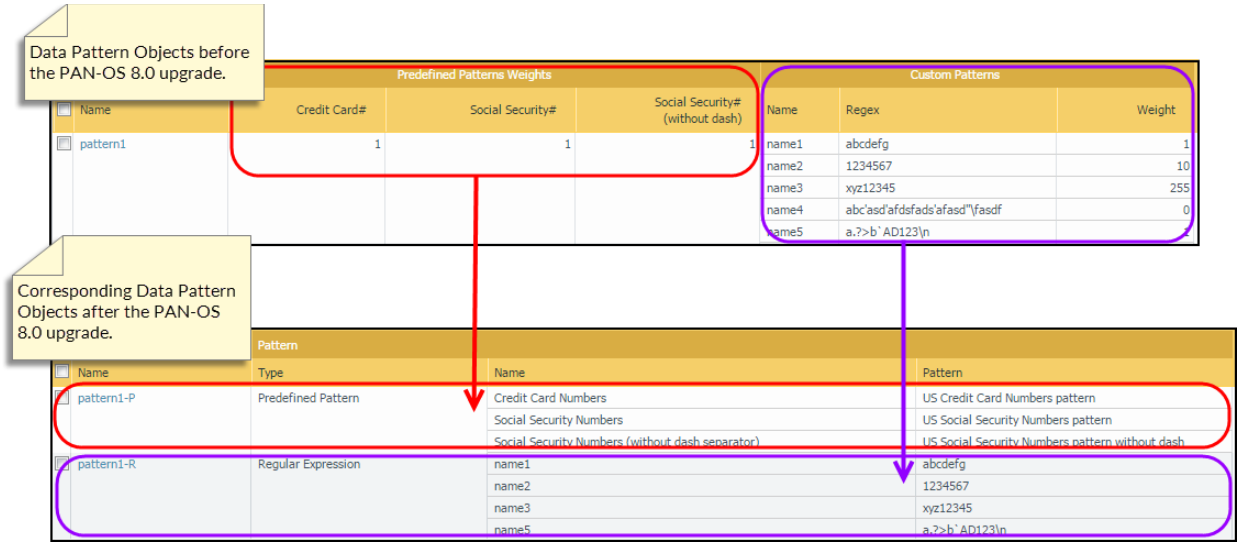
First Look at New and Updated Data Filtering Options

In previous release versions, a single data pattern object could contain different types of data patterns, including credit card and social security number patterns and custom patterns. Now, data pattern objects can be one of three types:

- (New & Improved) **Predefined Pattern**—Filter for credit card and social security numbers (with or without dashes) using predefined patterns. While the option to filter for credit card and social security numbers existing in previous release versions, the new predefined patterns make this feature easy to use.
- **Regular Expression**—Filter for a string of characters.
- (New & Improved) **File Properties**—Filter for file properties and values based on file type. While the option to use regular expression patterns to filter for file properties is supported with earlier release versions, the new built-in file property options make this feature easy to use.



Additionally, data pattern objects configured before the upgrade to PAN-OS 8.0 are preserved and are enforced with your security policy just as they were before the upgrade; however, the migrated data pattern objects are displayed differently. A single data pattern object that contains more than one *type* of pattern becomes two separate data pattern objects in PAN-OS 8.0:



In the example above, the PAN-OS 7.1 data pattern object *pattern1* includes credit card and social security number patterns and regular expression patterns. After the upgrade to PAN-OS 8.0, the original data pattern object is replaced by two separate objects based on the data pattern types: a predefined pattern object with the name *pattern-1P* and a regular expression object with the name *pattern1-R*.

A **P** added to the end of the data pattern name indicates a predefined data pattern that was configured before the upgrade to PAN-OS 8.0, and an **R** added to the end of the pattern name indicates a regular expression data pattern that was configured before the upgrade to PAN-OS 8.0.

Align Data Filtering with a DLP Solution

If you are using a DLP solution to add file properties to documents in order to mark those documents as confidential, you can use the new built-in file property settings to configure the firewall to block those confidential documents from leaving your network.

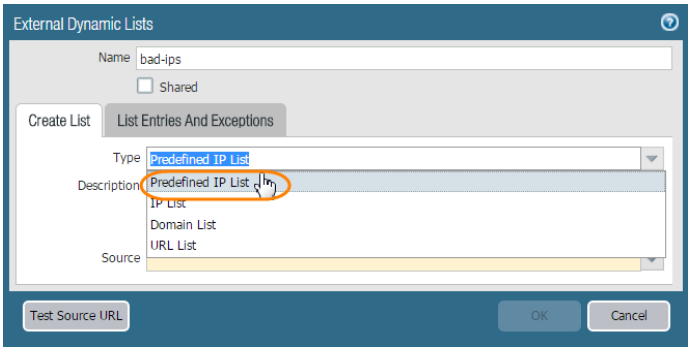
Take the following steps to use the new settings to enable data filtering based on file properties (previous release versions required you to create regular expression data patterns to enable the same functionality).

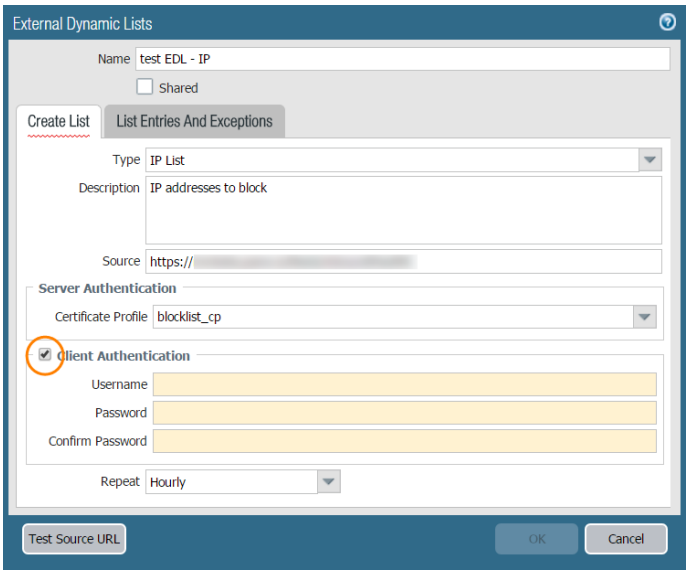
Filter Data Based on File Properties		
Step 1	Define a new data pattern object to detect file properties.	1. Select **Objects > Custom Objects > Data Patterns** and **Add** a new object. 2. Set the **Pattern Type** to **File Properties**. 3. **Add** a new rule to the data pattern object, and give that rule a descriptive Name. 4. Select the **File Type** and based on the file type you choose, also select the **File Property** that you want scan for a specific value. 5. Enter the specific **Property Value** that you want the firewall to detect. 6. Click **OK** to save the data pattern.
Step 2	Add the data pattern object to a data filtering profile.	1. Select **Objects > Security Profiles > Data Filtering** and **Add** or modify a data filtering profile. 2. **Add** a new profile rule and select the Data Pattern you created in Step 1. 3. Specify **Applications**, **File Types**, and what **Direction** of traffic (upload or download) you want to filter based on the data pattern. The file type you select must be the same file type you defined for the data pattern in Step 1, or it must be a file type that includes the data pattern file type. For example, you could define both the data pattern object and the data filtering profile to scan all Microsoft Office documents. Or, you could define the data pattern object to match to only Microsoft PowerPoint Presentations, while the data filtering profile scans all Microsoft Office documents. If a data pattern object is attached to a data filtering profile and the configured file types do not align between the two, the profile will not correctly filter documents matched to the data pattern object. 4. Set the **Alert Threshold** to specify the number of times the data pattern must be detected in a file to trigger an alert. 5. Set the **Block Threshold** to block files that contain at least this many instances of the data pattern. 6. Set the **Log Severity** recorded for files that match this rule. 7. Click **OK** to save the data filtering profile.

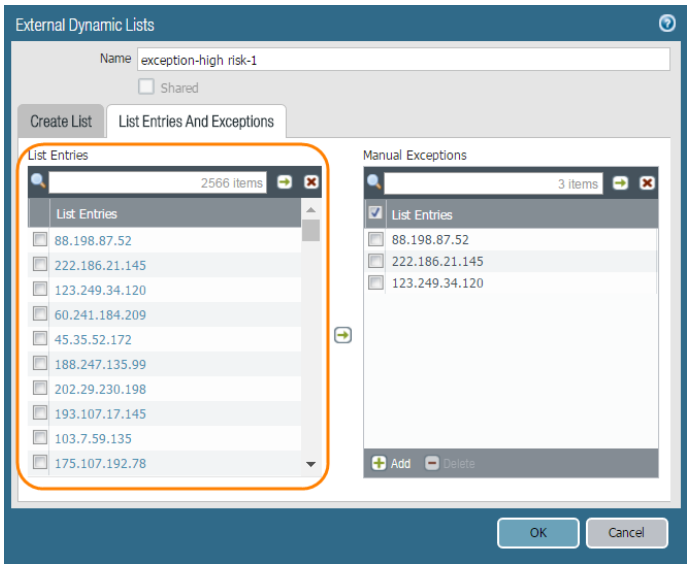
Filter Data Based on File Properties (Continued)		
Step 3	Apply the data filtering settings to traffic.	1. Select **Policies > Security** and **Add** or modify a security policy rule. 2. Select **Actions** and set the Profile Type to **Profiles**. 3. Attach the Data Filtering profile you created in Step 2 to the security policy rule. 4. Click **OK**.
Step 4	(Recommended) Prevent web browsers from resuming sessions that the firewall has terminated.  This option ensures that when the firewall detects and then drops a sensitive file, a web browser cannot resume the session in an attempt to retrieve the file.	1. Select **Device > Setup > Content-ID** and edit Content-ID Settings. 2. Clear the **Allow HTTP header range option**. 3. Click **OK**.
Step 5	Monitor files that the firewall is filtering.	Select **Monitor > Data Filtering** to view the files that the firewall has detected and blocked based on your data filtering settings.

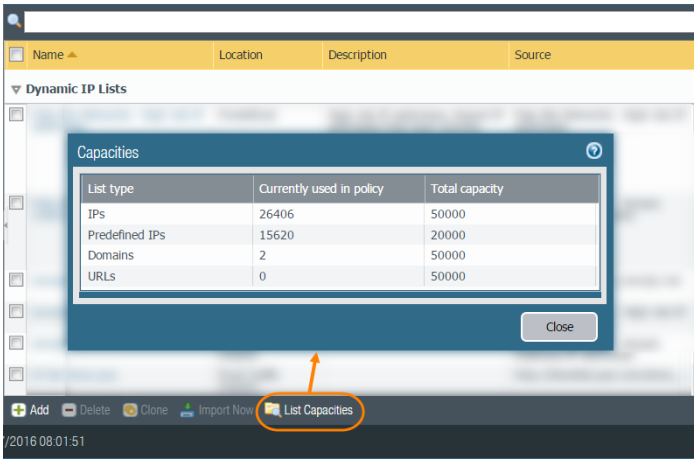
External Dynamic List Enhancements

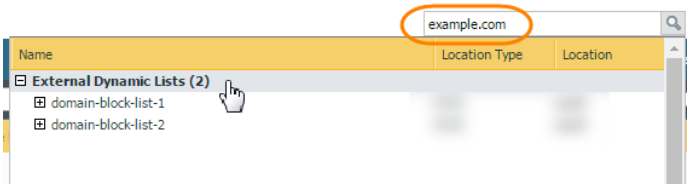
An external dynamic list is a text file of IP addresses, domains, or URLs hosted on an external web server. You can configure the firewall to periodically import an external dynamic list and block or allow traffic based on its contents. The following enhancements provide more visibility into the contents of an external dynamic list and the list entries currently used in policy. External dynamic lists also now give you the flexibility to choose list entries to exclude before using a list to enforce policy, while new authentication measures allow you to use external dynamic lists more securely. Lastly, you can now protect your network against malicious hosts by using new dynamic IP address lists that Palo Alto Networks maintains.

Explore New External Dynamic List Enhancements	
• Use one of the Palo Alto Networks Malicious IP Address Feeds as a source for the external dynamic list.	1. Select **Objects > External Dynamic List**. 2. Click **Add**. 3. When setting the details for the new external dynamic list, select the new external dynamic list Type **Predefined IP List**.  4. Select a Palo Alto Networks malicious IP address feed as the list Source. 5. Click **OK**.

Explore New External Dynamic List Enhancements (Continued)	
• Enable Authentication for External Dynamic Lists. Server authentication ensures that your firewall retrieves external dynamic lists from valid sources. Client authentication enables you to use external dynamic lists from more secure sources that require a username and password to restrict list access.	1. Select **Objects > External Dynamic List**. 2. Click on an external dynamic list to view the list settings. 3. Select a **Certificate Profile** for authenticating the web server that hosts the external dynamic list. 4. If the external dynamic list source requires a username and password to access the list, select **Client Authentication** and enter login credentials for the list.  5. Click **OK**.

Explore New External Dynamic List Enhancements (Continued)	
• View external dynamic list entries directly on the firewall.	1. Select **Objects > External Dynamic List**. 2. Click on an external dynamic list to view the list settings. 3. Click the **List Entries and Exceptions** tab. View the entries from the most recent version of the list that the firewall retrieved.  View AutoFocus threat intelligence for an external dynamic list entry to assess its pervasiveness and risk in your network. Click the drop-down next to a list entry, and click **AutoFocus**. To use this feature, you must have an active AutoFocus subscription and enable AutoFocus threat intelligence on the firewall.
• Exclude entries from an external dynamic list. This is useful if you want to block or allow traffic based on some but not all of the entries in a list.	1. View external dynamic list entries directly on the firewall. 2. Add an entry to the Manual Exceptions list. a. Select a list entry and click Submit ( ). b. Click **Add** and manually enter a value (refer to formatting guidelines for an external dynamic list). A manual exception must match a list entry exactly. For example, if one of the entries in an external dynamic list is the IP address range 1.1.1.1-3.3.3.3 and you manually enter 2.2.2.2 as an exception, the firewall will not consider it an exception unless 2.2.2.2 is also a list entry. You can add up to 100 exceptions to an external dynamic list. You cannot save your changes to the external dynamic list if you have duplicate entries in the list of exceptions. The firewall marks duplicate entries with a red underline.

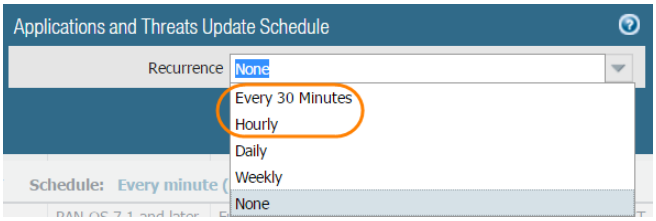
Explore New External Dynamic List Enhancements (Continued)	
• Check the number of external dynamic list entries used in policy to make sure you don't go over the firewall limit. In PAN-OS 8.0, you can reference a total of 30 external dynamic lists with unique sources across all security policy rules. In addition, external dynamic list entries (IP addresses, domain, and URLs) now only count toward the maximum number supported by the firewall if they belong to lists referenced in Security policy rules you enforce on the firewall.	1. Select **Objects > External Dynamic List**. 2. Click **List Capacities**. Compare how many IP addresses, domains, and URLs are currently used in policy against the total number of entries that the firewall supports for each list type. Since these values vary from firewall to firewall, the List Capacities window is not available on Panorama. Predefined IPs displays the number of IP addresses in the most recent Palo Alto Networks Malicious IP Address Feeds saved to your firewall, even if they are not used in policy. 

Explore New External Dynamic List Enhancements (Continued)	
• Use Global Find to check if a domain, IP address, or URL belongs to one or more external dynamic lists used in policy. This feature is useful for determining which external dynamic list (referenced in a Security policy rule) is causing the firewall to block or allow a certain domain, IP address, or URL. You can use Global Find from any page on the firewall.	1. Click **Search**. 2. Enter an IP address, domain, or URL, and click the spyglass to start the search. If you enter an IP address that falls within an IP address range entry in an external dynamic list, Global Find will not associate the IP address with the external dynamic list. For example, if you search for the IP address 2.2.2.2 and there is an external dynamic list with the entry 1.1.1.1-3.3.3.3, the search results for 2.2.2.2 do not include that external dynamic list. 3. If the IP address, domain, or URL is in an external dynamic list that is used in policy, the search results include the new category **External Dynamic Lists**. Expand this category to view which external dynamic lists contain the value you entered. If an IP address, domain, or URL is a list exception and you search for it in Global Find, the search results still include the external dynamic list(s) from which it is excluded. 

New Scheduling Options for Application and Threat Content Updates

The firewall can now check for the latest App-ID, vulnerability protection, and anti-spyware signatures every 30 minutes or hourly, in addition to being able to check for these updates daily and weekly. These new scheduling options mean that the firewall can retrieve Applications and Threats content updates within as little as 30 minutes of when the updates are made available. This enables more immediate coverage for newly-discovered threats and strengthens safe enablement for updated and newly-defined applications.

You can also use Panorama to set the schedule for managed firewalls to retrieve Applications and Threats content updates. Managed firewalls that are not upgraded to PAN-OS 8.0 will convert the 30-minute or hourly schedule to a daily schedule (and by default, they will check for new content updates at 3 AM daily).

Check for Application and Threat Updates Every 30 Minutes or Hourly		
Step 1	Confirm that the Threat Prevention license is active on the firewall. If you do not have a Threat Prevention license, but still want to the firewall to check for Application updates every 30 minutes, continue to Step 2.	Select **Device > Licenses** and check that the Threat Prevention license is active.
Step 2	Set the schedule for the firewall to retrieve Applications and Threats updates.	1. Select **Device > Dynamic Updates**. 2. Select the schedule link for Applications and Threats. 3. Set the **Recurrence** to **Every 30 Minutes** or **Hourly** for the firewall to check for new Applications and Threats every half hour or every hour.  4. Click **OK** to save the new Applications and Threats update schedule.

Five-Minute Updates for PAN-DB Malware and Phishing URL Categories

The Malware and Phishing URL categories in the PAN-DB cloud are now updated every five minutes based on the latest information from the Threat Intelligence cloud. Firewalls with an active PAN-DB URL Filtering license automatically benefit from these more frequent URL category updates following the upgrade to PAN-OS 8.0.

With PAN-DB URL Filtering, the firewall holds a cache of URLs and their categorizations locally; when a user accesses a website that is not in the local cache or if the local cache entry has expired, the firewall queries the PAN-DB cloud to determine the URL category of the website. At this time, the firewall will get the very latest categorization for the URL from the PAN-DB cloud, and will add the new URL to the local cache. To ensure that the firewall is configured to then block access to malware and phishing sites based on the latest URL category updates, take the following steps.

Block Malware and Phishing URL Categories		
Step 1	Enable PAN-DB URL Filtering.	This includes obtaining and installing a PAN-DB URL Filtering license and activating URL filtering.
Step 2	Restrict access to malicious and phishing sites.	1. Select **Objects > Security Profiles > URL Filtering** and **Add** or modify a URL filtering profile. Configure a best practice URL Filtering profile to ensure protection against URLs that have been observed hosting malware or exploitive content. 2. Select **Categories**. 3. Check that the Site Access for the malware and phishing categories is set to **block**. 4. Click **OK** to save the profile.
Step 3	(Optional) You can also enable the new Credential Phishing Prevention feature to prevent users from submitting credentials to untrusted sites, without blocking their access to those sites.	

Globally Unique Threat IDs

All Palo Alto Networks threat signatures now have permanent, globally unique IDs that you can use to look up threat signature information and create permanent threat exceptions. While globally unique IDs are already provided for vulnerability and spyware signatures, this release extends unique IDs to antivirus and DNS signatures. Previously, antivirus and DNS signature IDs were sometimes reused due to the large number of signatures generated on a daily basis and some IDs matched to more than one signature. Now, because you must configure threat exceptions based on threat IDs, globally unique threat IDs ensure that these exceptions remain permanently and correctly enforced.

Additionally, PAN-OS 8.0 introduces new threat categories to classify different types of threat signatures along with the new threat IDs. You can use the threat categories to filter both firewall logs and the ACC for certain types of threats and to build custom reports.

- ▲ Learn More About Threat Signatures using Threat IDs
- ▲ New Threat Categories and How to Use Them

Review the PAN-OS 8.0 upgrade and downgrade considerations for this feature before you get started:

- Because antivirus and DNS signatures now have globally unique IDs, the threat ID ranges that existed for these signatures in previous release versions no longer apply. If you have used antivirus and DNS threat ID ranges to build any custom logic, to create custom reports, or as part of an integration with a security information and event management (SIEM) solution, you should revisit those areas to see if you can instead leverage the new Threat categories.
- Threat exceptions configured in PAN-OS 7.1 are not migrated with the upgrade to PAN-OS 8.0. Instead, you can now use the new, permanent, and unique IDs to New Threat Categories and How to Use Them.

Learn More About Threat Signatures using Threat IDs

The firewall Threat logs record all threats the firewall detects based on threat signatures and the ACC displays an overview of the top threats on your network. Each event the firewall records includes an ID that identifies the associated threat signature.

Now that all threat IDs are unique, you can use the threat ID found with a Threat log or ACC entry to:

- ❒ Easily check if a threat signature is configured as an exception to your security policy.

What is a threat exception?

Palo Alto Networks defines a default action (such as block or alert) for threat signatures; unless otherwise specified, the firewall enforces threat signatures based on the default action. However, you can create a *threat exception* to either exclude a threat signature from enforcement or to modify how the firewall enforces that specific signature. Learn more about and create threat exceptions.

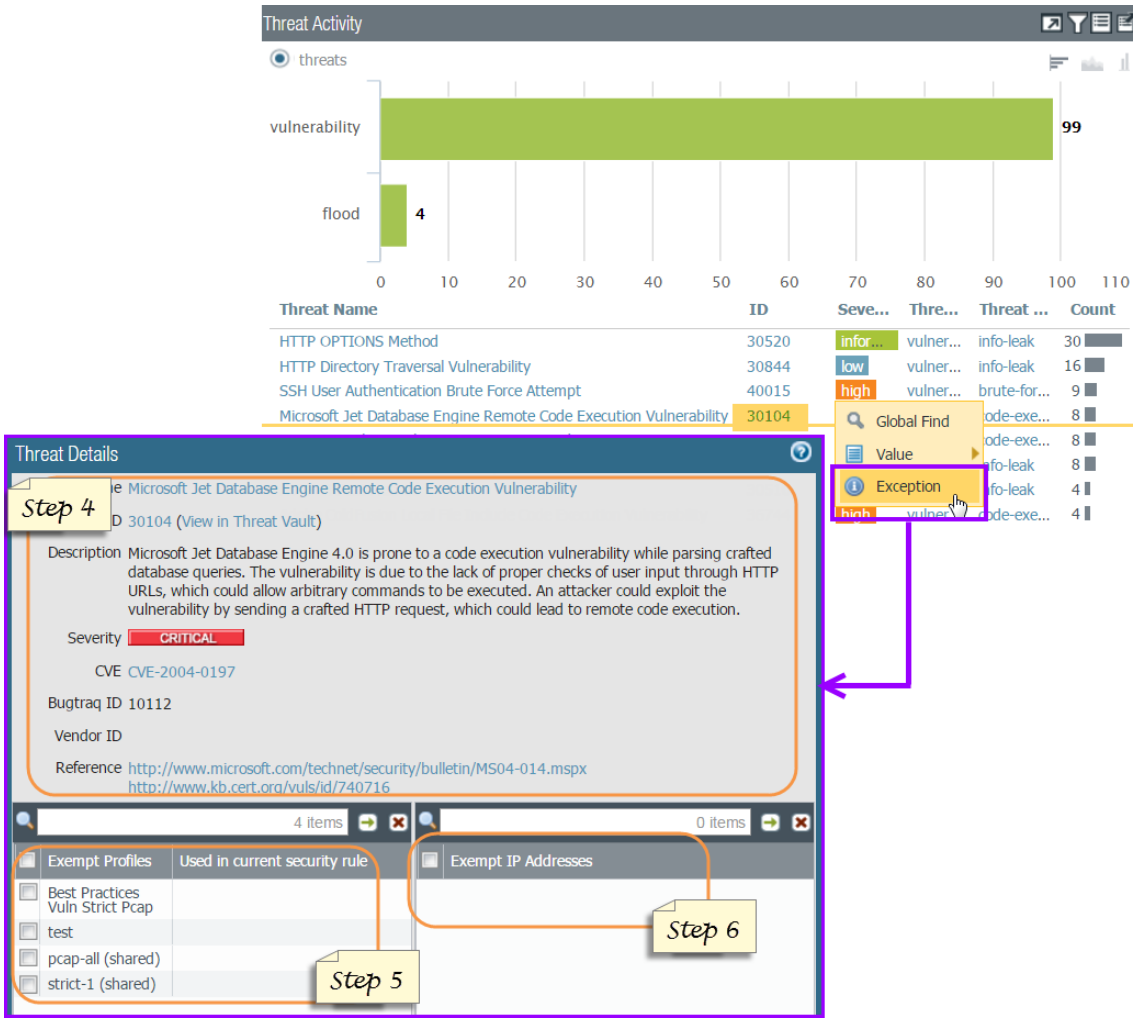
- ❒ Find the latest Threat Vault information about a specific threat. Because the Threat Vault is now integrated with the firewall, you can view threat details directly in the firewall context or launch a Threat Vault search in a new browser window for a threat the firewall logged.

Find Threat Details Using Threat IDs		
Step 1	Confirm the firewall is connected to the Threat Vault.	The firewall is now enabled to access the Threat Vault by default in order to gather the latest information about detected threats. To confirm that threat vault access is enabled after upgrading to PAN-OS 8.0, select **Device > Setup > Management** and edit the **Logging and Reporting** setting to **Enable Threat Vault Access**.
Step 2	Find the threat ID for threats the firewall detects: • To see each threat event the firewall detects based on threat signatures, select **Monitor > Logs > Threat**. You can find the ID for a threat entry listed in the ID column, or select the log entry to view log details, including the Threat ID. • To see an overview of top threats on the network, select **ACC > Threat Activity** and take a look at the Threat Activity widget. The ID column displays the threat ID for each threat displayed. • To see details for threats that you can configure as threat exceptions (meaning, the firewall enforces the threat differently than the default action defined for the threat signature), select **Objects > Security Profiles > Anti-Spyware/Vulnerability Protection**. **Add** or modify a profile and click the **Exceptions** tab to view configured exceptions. If no exceptions are configured, you can filter for threat signatures or select **Show all signatures**.	

Find Threat Details Using Threat IDs (Continued)

Step 3 Hover over a **Threat Name** or the threat **ID** and click **Exception** to review both the threat details and how the firewall is configured to enforce the threat.

For example, find out more about a top threat charted on the ACC:



Step 4 Review the latest **Threat Details** for the threat and launch a Threat Vault search based on the threat ID:

- Threat details displayed include the latest Threat Vault information for the threat, resources you can use to learn more about the threat, and CVEs associated with the threat.
- Select **View in Threat Vault** to open a Threat Vault search in a new window and look up the latest information the Palo Alto Networks threat database has for this threat signature.

Find Threat Details Using Threat IDs (Continued)	
Step 5	Check if a threat signature is configured as an exception to your security policy: • If the **Used in current security rule** column is clear, the firewall is enforcing the threat based on the recommended default signature action (for example, block or alert). • A checkmark anywhere in the **Used in current security rule** column indicates that a security policy rule is configured to enforce a non-default action for the threat (for example, allow), based on the associated **Exempt Profiles** settings. The **Used in security rule column** does not indicate if the security rule is enabled, only if the security policy rule is configured with the threat exception. Select **Policies > Security** to check if an indicated security policy rule is enabled.
Step 6	**Add** an IP address on which to filter the threat exception or view existing **Exempt IP Addresses**. Configure an exempt IP address to enforce a threat exception only when the associated session has either a matching source or destination IP address; for all other sessions, the threat is enforced based on the default signature action.

New Threat Categories and How to Use Them

This feature also introduces new threat categories to classify different types of threats. You can use threat categories to filter threat logs and ACC activity and to build custom reports. If, in earlier release versions, you had configured custom reports for antivirus and DNS signatures based on threat ID ranges, you can use threat categories to recreate those reports.

Custom reports based on antivirus and DNS ID ranges will no longer exist following the upgrade to PAN-OS 8.0.

The following table lists and describes threat categories that are used to classify different types of threat signatures and the events that these signatures detect. The threat categories are subsets of the more broad threat signature types: spyware, vulnerability, antivirus, and DNS signatures.

New Threat Category in PAN-OS 8.0	Description	Threat Type	Content Update that Provides These Signatures
apk	Malicious Android Application Package (APK) files.	virus wildfire-virus	Antivirus WildFire or WildFire Private
autogen	C2 traffic that has been detected with automatically-generated C2 signatures—these signatures can detect C2 traffic even when the C2 host is unknown or changes rapidly.	spyware	Antivirus
dmg	Apple disk image files (DMG), used with the Mac OS X operating system.	virus wildfire-virus	Antivirus WildFire or WildFire Private
dns	DNS queries for hostnames associated with malware.	spyware	Antivirus

New Threat Category in PAN-OS 8.0	Description	Threat Type	Content Update that Provides These Signatures
dns-wildfire	DNS queries for hostnames associated with malware—these are queries that WildFire detected when executing a previously unknown file in the WildFire virtual environment.	spyware	WildFire or WildFire Private
flash	Adobe Flash applets and Flash content embedded in web pages.	virus wildfire-virus	Antivirus WildFire or WildFire Private
flash-lzma	Adobe flash files that have undergone Lempel-Ziv-Markov chain algorithm (LZMA) compression.	virus wildfire-virus	Antivirus WildFire or WildFire Private
java-class	Java applets (JAR/class file types).	virus wildfire-virus	Applications and Threats
js	JavaScript files.	virus	Antivirus
macho	Mach object files (Mach-O) are executables, libraries, and object code that are native to the Mach OS X operating system.	virus wildfire-virus	Antivirus WildFire or WildFire Private
office	Microsoft Office files, including documents (DOC, DOCX, RTF), workbooks (XLS, XLSX), and PowerPoint presentations (PPT, PPTX).	virus wildfire-virus	Antivirus WildFire or WildFire Private
openoffice	Office Open XML (OOXML) 2007+ documents.	virus wildfire-virus	Antivirus WildFire or WildFire Private
pdf	Portable Document Format (PDF) files.	virus wildfire-virus	Antivirus WildFire or WildFire Private
pe	Portable Executable (PE) files, including object code, DLLs, and FON (fonts).	virus wildfire-virus	Antivirus WildFire or WildFire Private
pkg	Apple software installer packages (PKGs), used with the Mac OS X operating system.	virus wildfire-virus	Antivirus WildFire or WildFire Private

Predefined File Blocking Profiles

You can now quickly and easily enforce the best practice file blocking settings on your Security policy allow rules using two new predefined File Blocking profiles. For most traffic (including traffic on your internal network) you will want to block files that are known to carry threats or that have no real use case for upload/download to ensure that malware is not sneaking into your network or that sensitive data is not being exfiltrated out of your network in legitimate traffic.

The new profiles are intended a starting point that you can use to clone and modify per your specific business requirements:

- **basic file blocking**—Attach this profile to the Security policy rules that allow traffic to and from less sensitive applications to block files that are commonly included in malware attack campaigns or that have no real use case for upload/download. It blocks upload and download of PE files (.scr, .cpl, .dll, .ocx, .pif, .exe) , Java files (.class, .jar), Help files (.chm, .hlp) and other potentially malicious file types, including .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat. Additionally, it prompts users to acknowledge when they attempt to download encrypted-rar or encrypted-zip files. This rule alerts on all other file types to give you complete visibility into all file types coming in and out of your network.
- **strict file blocking**—Use this stricter profile on the Security policy rules that allow access to your most sensitive applications. This profile blocks the same file types as the other profile, and additionally blocks flash, .tar, multi-level encoding, .cab, .msi, encrypted-rar, and encrypted-zip files.

Name	Location	Rule Name	Applications	File Types	Direction	Action
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, msi, multi-level-encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert

WildFire Features

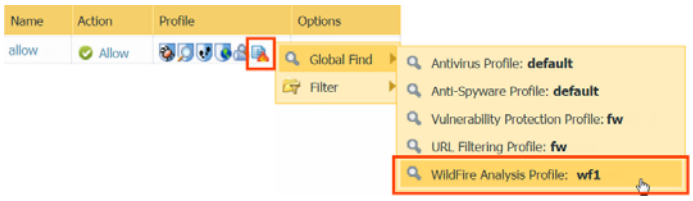
- WildFire Phishing Verdict
- WildFire Analysis of Blocked Files
- Panorama Centralized Management for WildFire Appliances
- WildFire Appliance Clusters
- Preferred Analysis for Documents or Executables
- Verdict Changes
- Verdict Checks with the WildFire Global Cloud

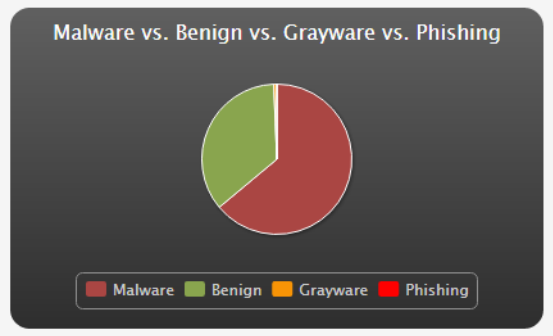
WildFire Phishing Verdict

The new WildFire phishing verdict classifies credential phishing links found in emails separately from emailed links found to be exploits or malware. When the firewall detects a link in an email, it forwards the link to WildFire for analysis. WildFire classifies the link as phishing based on properties and behaviors the accompanying website displays and assigns the link the new phishing verdict. Phishing links are logged as WildFire Submissions to indicate that the firewall detected such a link in an email.

Firewalls with an active WildFire license that are connected to the WildFire public cloud and are configured to forward email links for analysis will automatically start receiving phishing verdicts after the upgrade to PAN-OS 8.0. Firewalls with both a WildFire license and a PAN-DB URL Filtering license can block access to phishing sites within five minutes of initial discovery.

For Firewalls in a WildFire Private Cloud Deployment:
The WildFire appliance does not support the new Phishing verdict. However, firewalls connected to a WildFire appliance that also have an active PAN-DB URL Filtering license can still benefit from phishing protection. For these firewalls, continue to Step 5 to block users from accessing newly-discovered phishing sites.

Get Phishing Verdicts and Block Access to Phishing Sites	
Step 1 Check that the firewall has an active WildFire license and is connected to WildFire. Blocking access to phishing sites requires a PAN-DB URL Filtering license, in addition to the WildFire license.	1. Select **Device > Licenses** to confirm that the WildFire License is active. If you are also planning to block access to phishing sites, confirm that the PAN-DB URL Filtering license is active. 2. Select **Device > Setup > WildFire** and confirm that the **WildFire Public Cloud** field is set to `wildfire.paloaltonetworks.com`. 3. Alternatively, you can connect the firewall to a WildFire regional cloud in the European Union (EU) or in Japan.
Step 2 Verify that the firewall is enabled to forward email links for WildFire analysis.	1. Select **Objects > Security Profiles > WildFire Analysis** and confirm that at least one profile is configured to forward **email-link** or **any** File Types for WildFire analysis. 2. Select **Policies > Security** to confirm that the WildFire Analysis profile is attached to a security policy rule: 

Get Phishing Verdicts and Block Access to Phishing Sites (Continued)		
Step 3	Monitor phishing links.	• View links the firewall forwarded that WildFire found to be phishing links: Select **Monitor > WildFire Submissions**. The Verdict column displays Phishing for entries that record a phishing link. You can add the following filter to display only logs for phishing links: `(verdict eq phishing)`. • View phishing activity on the firewall ACC: Select **ACC > Threat Activity**, view WildFire Activity By Type and select **phishing**. • View all phishing links WildFire has identified: The WildFire portal displays the total number of WildFire submissions that were found to be phishing links in the last hour and the last 24 hours:  Select **Reports**, filter by **Verdict**, and select **Phishing** to find the analysis reports for phishing links. If you are submitting links to a regional WildFire cloud for analysis, instead use the WildFire EU portal or the WildFire Japan portal.
Step 4	Forward phishing logs as SNMP traps, syslog messages, or email notifications.	1. Select **Objects > Log Forwarding** and **Add** or modify a log forwarding profile to define the logs you want to forward. 2. **Add** a rule to the profile. 3. Set the **Log Type** to wildfire. 4. Add the **Filter** `( verdict eq phishing )`. 5. Continue to define or update the profile, and click **OK** to save the profile when you're done. 6. Apply the new or updated log forwarding settings to traffic: a. Select **Policies > Security** and **Add** or modify a security policy rule. b. Select **Actions** and in the Log Setting section, attach the new or updated **Log Forwarding** profile to the security policy rule. c. Click **OK** to save the security policy rule.

Get Phishing Verdicts and Block Access to Phishing Sites (Continued)		
Step 5	(Optional) To prevent users from inadvertently leaking corporate credentials to attackers, block access to phishing sites and block users from submitting usernames and passwords to untrusted and unsanctioned sites.	1. Select **Objects > URL Filtering** and **Add** or modify a URL Filtering profile. 2. Select **Categories** and filter the list of URL categories to find the phishing category. 3. Set the **Site Access** for phishing websites to **Block** to prevent users from accessing sites that aim to steal usernames and passwords. 4. Enable the new Credential Phishing Prevention feature to stop users from submitting credentials to untrusted sites, without blocking their access to these sites. 5. Apply the new or updated URL Filtering profile to traffic: a. Select **Policies > Security** and **Add** or modify a security policy rule. b. Select **Actions** and in the Profile Setting section, set the **Profile Type** to profiles. c. Attach the new or updated **URL Filtering** profile to the security policy rule. d. Click **OK** to save the security policy rule.

WildFire Analysis of Blocked Files

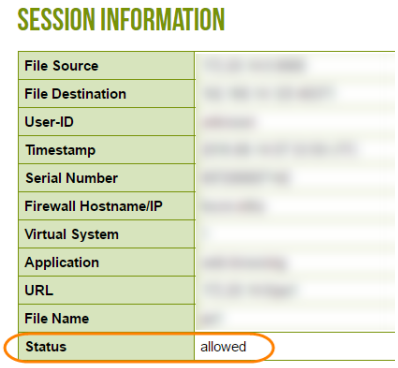
If you enabled WildFire forwarding on your firewall, the firewall now submits blocked files that match antivirus signatures for WildFire analysis, in addition to unknown files. This allows WildFire to extract valuable information from new malware variants. Malware signatures often match multiple variants of the same malware family, and as such, block new malware variants that the firewall has never seen before. Sending these blocked malware samples for WildFire analysis allows WildFire to analyze them for additional URLs, domain names, and IP addresses that must be blocked. Since all WildFire analysis data is also available on AutoFocus, you can now use WildFire and AutoFocus to get a more complete perspective of all threats targeting your network, including blocked threats; this improves the efficacy of your security operations, incident response, and threat analysis.

Because blocked files are now forwarded to WildFire for analysis, you now have visibility into files that the firewall has successfully blocked. On the firewall, you can now view WildFire Submissions log details for blocked files, which include the threat log entry for a file and the threat ID matched to a file (for more information, refer to Globally Unique Threat IDs). Both the firewall and the WildFire portal also provide access to the WildFire analysis report for a blocked file so you can learn about its behavior when it executed in a WildFire analysis environment.

The firewall forwards blocked files to the WildFire public cloud based on your existing WildFire forwarding settings (**Objects > Security Profiles > WildFire Analysis**). The firewall doesn't forward files that are blocked based on your file blocking settings.

View Blocked Files

View Blocked Files		
Step 1	Verify that your firewall can forward files to WildFire.	If you have a WildFire license, verify that it is active on the firewall, and get started with WildFire. If you don't have a WildFire subscription, you can forward unknown and blocked files in portable executable (PE) format for WildFire analysis.

View Blocked Files (Continued)	
Step 2 View blocked files and their WildFire analysis information. The firewall and the WildFire portal do not generate email alerts for blocked files.	On the firewall, select **Monitor > Logs > WildFire Submissions**, and choose from the following options: • To check whether a file was allowed or blocked by the firewall, view the Action column. WildFire submissions prior to PAN-OS 8.0 display with the firewall action **alert**. Now, for files forwarded to WildFire after upgrading to PAN-OS 8.0, the action displayed is either **allow** or **block**. Log entries with the action **allow** are files that the firewall has allowed to pass through your network. They can be known files that are benign or files allowed by your security policies. Log entries with the action **block** are files that the firewall has blocked based on antivirus signatures. • To view only blocked files in the WildFire Submissions log, construct the filter `(action eq block)` and click Apply Filter. Refer to the complete workflow for filtering logs. • To view the WildFire file analysis details for a blocked file, click the spyglass ( ) next to the log entry and view the **WildFire Analysis Report** tab. Alternatively, view blocked files on the WildFire portal: 1. Log in to the WildFire portal (https://wildfire.paloaltonetworks.com) with your support account credentials. 2. On the dashboard, choose one of the following actions: • Select a **Source** to view a list of files uploaded to WildFire by a particular source. • Click **Reports** to view all files uploaded to WildFire. 3. Click report icon to view the WildFire analysis report for a file. 4. Under Session Information, view the file Status to check whether the file was **allowed** or **blocked** by the firewall.  SESSION INFORMATION File Source File Destination User-ID Timestamp Serial Number Firewall Hostname/IP Virtual System Application URL File Name Status allowed The file Status is not available for files uploaded manually to the WildFire portal or with the WildFire API.
Step 3 Continue investigating blocked files.	• Use the SHA-256 hash (now provided for a blocked file that match antivirus signatures) to view artifacts associated with a blocked file in AutoFocus or VirusTotal. • Use Globally Unique Threat IDs, found in the log entry for a blocked file, to search Threat Vault for the name of the signature that blocked the file.

Panorama Centralized Management for WildFire Appliances

Beginning with release 8.0.1, you can now manage WildFire appliances and WildFire appliance clusters with Panorama. Panorama can manage up to 200 WildFire appliances as WildFire appliance cluster nodes, standalone WF-500 appliances, or a combination of cluster nodes and standalone appliances. Panorama can manage a maximum of ten WildFire appliance clusters.

Compared to managing WildFire appliances and appliance clusters individually using the local CLI, using Panorama provides centralized management and monitoring of multiple appliances and appliance clusters. Centralized management enables you to push common configurations, configuration updates, and software upgrades to all or a subset of the managed WildFire appliances, which makes it easy to ensure that WildFire appliances and appliance clusters have consistent configurations.

WildFire Appliance Clusters

Beginning with this release, you can now configure and manage up to twenty WildFire appliances as a *WildFire appliance cluster* on a single network. This is especially useful in environments where you cannot use the WildFire public cloud. WildFire appliance clusters support larger firewall deployments on a single network than a standalone WildFire appliance supports. Additionally, clusters provide fault tolerance and a single signature package that is distributed to all firewalls that are connected to the cluster.

You can manage clusters locally, using the WildFire appliance CLI, or centrally, from a Panorama M-Series or virtual appliance. A WildFire cluster environment includes:

- From 2 to 20 WildFire appliances that you want to group and manage as a cluster. At a minimum, a cluster must have two WildFire appliances configured in a high-availability (HA) pair.
- Firewalls that connect to the cluster for traffic analysis and signature generation.
- (**Optional**) One or two Panorama appliances for centralized cluster management if you choose not to manage the cluster locally. To provide HA, use two Panorama appliances configured as an HA pair.

At a minimum, a cluster must have two WildFire appliances configured as a high-availability (HA) pair. WildFire appliances that you add to a WildFire appliance cluster become cluster nodes.

Configure a WildFire Appliance Cluster		
Step 1	Create a WildFire appliance cluster and add WildFire appliances to the cluster.	Configure the cluster member nodes and roles, configure HA, and verify the configuration. You can Configure a Cluster and Add Nodes Locally or Configure a Cluster and Add Nodes on Panorama.
Step 2	Configure basic WildFire appliance cluster settings.	Configure the connection to the WildFire public cloud, data retention policies, signature generation, the preferred analysis environment, DNS settings, and so on. You can Configure Basic Cluster Settings Locally or Configure Basic Cluster Settings on Panorama.
Step 3	Remove a WildFire appliance from a cluster.	Safely remove a node from a WildFire appliance cluster. You can Remove a Node from a Cluster Locally, however, removing a node from a cluster using Panorama is not supported.

With the introduction of managing WildFire appliance clusters on Panorama, you can also manage individual standalone WildFire appliances on Panorama.

Preferred Analysis for Documents or Executables

A single virtual machine (VM) image runs on the WildFire appliance; when you Upgrade the WildFire Appliance Software, you can choose for the WildFire appliance to use the VM image that most reflects your network environment. Each available VM image represents a single operating system and supports several different analysis environments based on that operating system. You can now dedicate all analysis environments to support certain file types: either documents (Microsoft Office files and PDFs) or portable executables (PEs). This feature is helpful if you are using the WildFire appliance to analyze specific file types; for example, if you've deployed a WildFire hybrid cloud to analyze documents locally and PEs in the WildFire global cloud. In this case, you could dedicate all analysis environments to documents. Previously, analysis environments were statically allocated and the resources available for document and executable analysis were evenly divided; you could not adjust the allocation of analysis resources even when the WildFire appliance was configured to analyze only one type of file.

Allocate WildFire Analysis Resources Based on File Type		
Step 1	Confirm that the firewall is configured to forward only the file type to which you want to dedicate WildFire analysis environments.	1. In the firewall web interface, select **Objects > Security Profiles > WildFire Analysis**. 2. Confirm that the WildFire Analysis profile set to forward files to the WildFire **private cloud** for analysis is configured to forward documents or executables. 3. Select **Policies > Security** and confirm that the WildFire Analysis profile is attached to a security policy rule. Traffic the rule allows is forwarded to the WildFire appliance for private cloud analysis based on the WildFire Analysis profile settings.
Step 2	Allocate WildFire appliance resources to analyze either documents or executables.	Use the following CLI command: `admin@WF-500# set deviceconfig setting wildfire preferred-analysis-environment documents | executables | default` and choose from one of the following options: • documents—Dedicate analysis resources to concurrently analyze 25 documents, 1 PE, and 2 email links. • executables—Dedicate analysis resources to concurrently analyze 25 PEs, 1 documents, and 2 email links. • default—The appliance concurrently analyzes 16 documents, 10 portable executables (PE), and 2 email links.
Step 3	Confirm that all WildFire appliances processes are running.	`admin@WF-500> show system software status`

Verdict Changes

You can now use the WildFire appliance to change a verdict for a sample. Verdict changes apply only to those samples submitted to the WildFire appliance, and the verdict for the same sample remains unchanged in the WildFire global cloud.

The WildFire private cloud content package is updated to reflect any verdict changes that you make (on the firewall, select **Device > Dynamic Updates > WF-Private** to enable WildFire private cloud content updates). When you change a sample verdict to malicious, the WildFire appliance generates a new signature to detect the malware and adds that signature to the WildFire private cloud content package. When you change a sample verdict to benign, the WildFire appliance removes the signature from the WildFire private cloud content package.

Change a WildFire Appliance Verdict

- **Change a sample verdict:**
  `admin@WF-500# submit wildfire local-verdict-change hash <sha256 hash> comment <comment> verdict <verdict>`
  - `hash`—Provide the SHA-256 hash of the file for which you want to change the verdict.
  - `verdict`—Enter the new file verdict: 0 indicates a benign sample; 1 indicates malware; 2 indicates grayware, and 4 indicates phishing.
  - `comment`—Include a comment to describe the verdict change.

- **See samples with changed verdicts:**
  `admin@WF-500# show wildfire global local-verdict-change all | <sha256 hash>`
  - `all`—See all samples with changed verdicts. The output includes the original verdict and the new verdict.
  - `<sha256 hash>`—Check a specific sample for a changed verdict. The output includes the original verdict and the new verdict.

- **Use the API to change a sample verdict:**
  Make a request to the new resource `submit/local-verdict-change` and include the API key, the file hash, the new verdict you want to apply to the sample, and a descriptive comment of the change:
  ```
  curl -X POST -H "Content-Type: multipart/form-data" -F "apikey=apikey" -F "hash=sha-256-hash" -F "verdict=0" -F "comment=comment-for-verdict-change" "https://wf-500/publicapi/submit/local-verdict-change"
  ```
  Use the following parameters when changing a WildFire appliance verdict for a file:
  - `apikey`—Enter your API key.
  - `hash`—Provide the SHA-256 hash of the file for which you want to change the verdict.
  - `verdict`—Enter the new file verdict: 0 indicates a benign sample, 1 indicates malware, 2 indicates grayware, and 4 indicates phishing.
  - `comment`—Include a comment to describe the verdict change.

  The following XML response verifies a successful verdict change. Example:
  ```
  <wildfire>
    <body>verdict is changed (old verdict: 0, new verdict:1)</body>
    <headers/>
  </wildfire>
  ```


Change a WildFire Appliance Verdict

- **Use the API to see samples with changed verdicts:**
  Make a request to the new resource `get/verdicts/changed` and include the API key and a start date for the query. Samples with changed verdicts from the specified start date to the present date is shown in this list:

```
curl -F "apikey=apikey" -F "date=YYYY-MM-DD" "https://wf-500/publicapi/get/verdicts/changed"
```

  The `verdict` element value can be one of the following:
  - `0`—benign
  - `1`—malware
  - `2`—grayware
  - `4`—phishing

  The XML response contains the WildFire verdict along with the related hash values for each sample with changed verdicts within the specified time-frame. Example:

```
<wildfire>
   <get-verdict-info>
       <sha256>afe6b95ad95bc689c356f34ec8d9094c495e4af57c932ac413b65ef132063acc</sha256>
       <verdict>1</verdict>
       <md5>0e4e3c2d84a9bc726a50b3c91346fbb1</md5>
   </get-verdict-info>
...........
   <get-verdict-info>
       <sha256>9739eb4207fe251d40f05187cbfd16081f97b246ebcc6010660244a84a9391b0</sha256>
       <verdict>2</verdict>
       <md5>481e625e50211efcaf6edb8f54f8cf83</md5>
   </get-verdict-info>
</wildfire>
```

Verdict Checks with the WildFire Global Cloud

The WildFire appliance can now leverage WildFire global cloud intelligence to deliver quick verdicts for known samples. This allows the WildFire appliance to dedicate analysis resources to samples that are truly unknown to both your private network and the global WildFire community. Before analyzing a sample locally, the WildFire appliance checks if the WildFire global cloud has already analyzed the sample (the WildFire appliance sends only the sample hash to the WildFire global cloud—it does not send the raw file or any additional sample data). If the sample is known to the WildFire global cloud, the WildFire appliance retrieves the sample verdict and analysis report and delivers them promptly to the firewall that detected the sample. If the sample is unknown to the WildFire global cloud, the WildFire appliance analyzes the sample locally. In either case, the WildFire appliance locally generates a signature to detect the malware, and delivers the signature to the firewall as part of the WildFire private cloud content update.

The WildFire appliance continues to periodically synchronize verdicts and analysis reports for locally-analyzed samples so that they match the verdicts and analysis reports the WildFire global cloud provides—this ensures that analysis information for locally-analyzed samples stays up-to-date with worldwide WildFire submissions and the latest threat intelligence. In cases where the WildFire global cloud and the WildFire appliance record a different verdict for a sample, the WildFire global cloud verdict takes precedence and changes the local verdict.

The following CLI command enables the WildFire appliance to perform verdict lookups and synchronize verdicts with the WildFire global cloud. This feature is disabled by default; set the command to `yes` to enable the feature.

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence cloud-query yes | no
```

Another new WildFire appliance feature supports Verdict Changes for locally-analyzed samples. If you change the verdict for a sample, the new verdict continues to apply to the locally-submitted sample, even if the WildFire global cloud has recorded a different verdict for the same sample.

Authentication Features

SAML 2.0 Authentication

You can now use Security Assertion Markup Language (SAML) 2.0 to authenticate administrators who access the firewall or Panorama web interface and end users who access services or applications. In environments where each user accesses many services or applications and authenticating for each one would impede user productivity, you can configure SAML single sign-on (SSO) to enable one login to access multiple services and applications. Likewise, SAML single logout (SLO) enables a user to end sessions for multiple services and applications by logging out of just one session. You can use SAML authentication for services and applications that are external or internal to your organization.

SSO is available to administrators and to GlobalProtect and Captive Portal end users. SLO is available to administrators and GlobalProtect end users, but not to Captive Portal end users.
Administrators can use SAML to authenticate to the firewall or Panorama web interface, but not to the CLI.

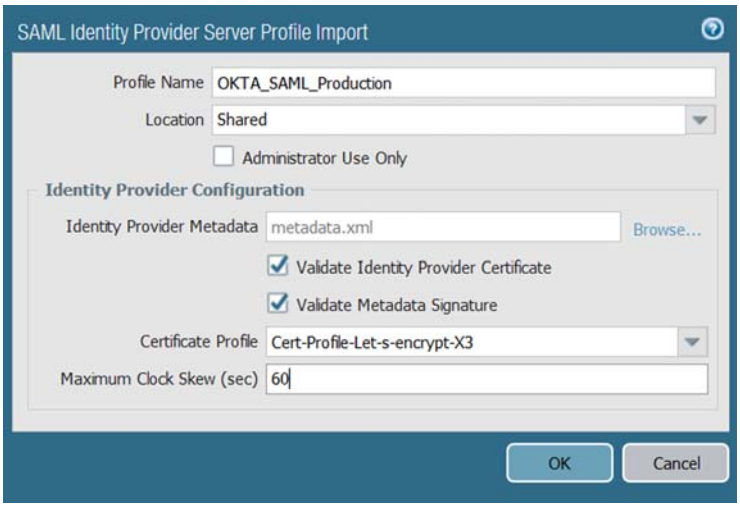
SAML authentication requires a service provider (the firewall or Panorama), which controls access to services or applications, and an identity provider (IdP) such as PingFederate, which authenticates users. To configure SAML authentication, you must register the firewall or Panorama and the IdP with each other to enable communication between them. If the IdP provides a metadata file containing registration information, you can import it onto the firewall or Panorama to register the IdP and to create an IdP server profile. The server profile specifies the certificate that the IdP uses to sign SAML messages. You can also import a certificate for the firewall or Panorama to sign SAML messages. Using certificates is optional but recommended to secure communications between the firewall or Panorama and the IdP.

Configure SAML Authentication	
Step 1	**(Recommended)** Obtain the certificate that the firewall will use to sign SAML messages that it sends to the IdP. If the certificate doesn't specify key usage attributes, all usages are allowed by default, including signing messages. In this case, you can obtain the certificates by any method. If the certificate does specify key usage attributes, one of the attributes must be Digital Signature, which is not available on certificates that you generate on the firewall or Panorama. In this case, you must import the certificate from your enterprise certificate authority (CA) or a third-party CA.

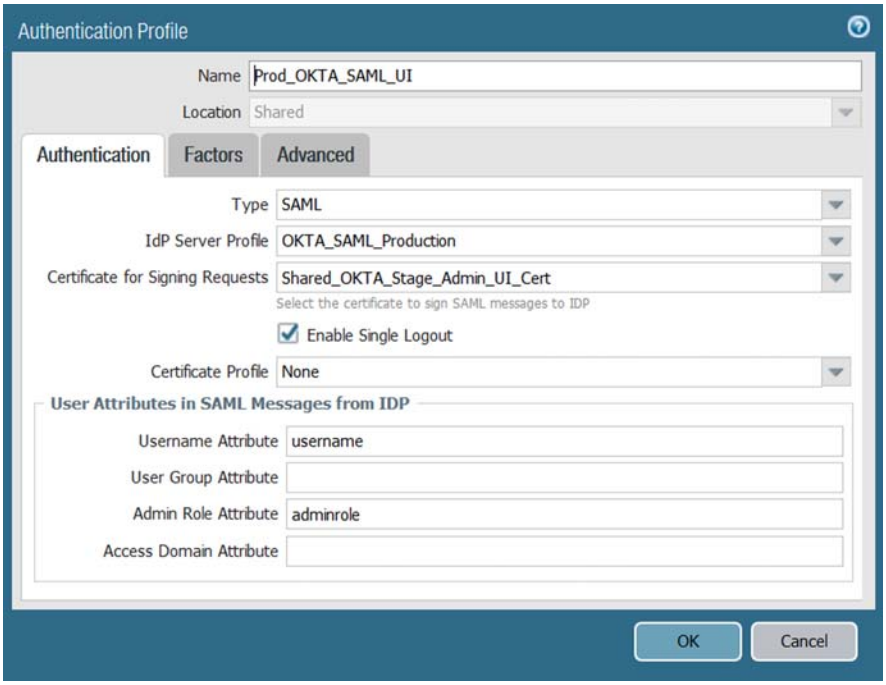
Configure SAML Authentication (Continued)

Step 2 Select **Device > Server Profiles > SAML Identity Provider** and **Import** the metadata file that your IdP provided.

When you import the metadata file, the firewall automatically creates a server profile and populates the connection, registration, and certificate information. The IdP uses the certificate to sign SAML messages that it sends to the firewall. You must manually configure the other server profile settings.



Step 3 Select **Device > Authentication Profile** and **Add** an authentication profile to define authentication settings such as SAML SLO. Select the **IdP Server Profile** you configured and select the **Certificate for Signing Requests**. The firewall uses this certificate to sign SAML messages that it sends to the IdP.



Configure SAML Authentication (Continued)

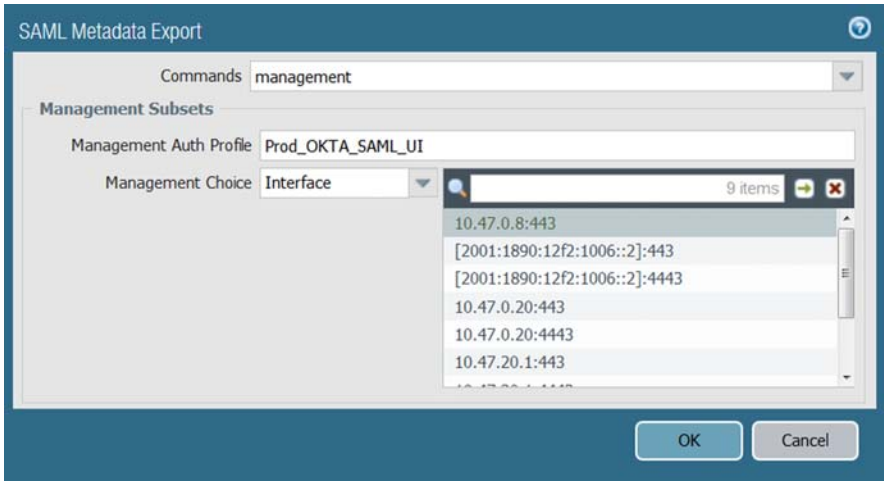
Step 4 Assign the authentication profile to firewall applications that require authentication.

- Administrator accounts that you manage locally on the firewall. In this example, create a local administrator before you verify the SAML configuration later in this procedure.
- Administrator accounts that you manage externally in the IdP identity store. Select **Device > Setup > Management**, edit the Authentication Settings, and select the **Authentication Profile**.
- Authentication policy rules that secure the services and applications that Captive Portal end users access.
- GlobalProtect portals and gateways that end users access.

Step 5 **Commit** your changes.

The firewall validates the **Identity Provider Certificate** that you assigned to the SAML IdP server profile.

Step 6 Create a metadata file that you can use to register the firewall application with the IdP—Select **Device > Authentication Profile** and click **Metadata** in the row of the authentication profile you configured.



Refer to your IdP documentation for the steps to import the metadata file onto the IdP server and register the firewall application.

Step 7 Verify that users can authenticate using SAML—As the administrator you created locally on the firewall, log in to the firewall web interface using the **Use Single Sign-On** option. After authenticating through the IdP, use the same administrator account to access another SSO application. If you can access the application without authenticating again (assuming Security policy allows access to that application), SSO authentication succeeded.

Authentication Policy and Multi-Factor Authentication

To protect services and applications from attackers, you can use the new Authentication policy to control access for end users. Authentication policy provides the benefit of letting you to choose how many authentication challenges of different types (factors) users must respond to. Using multiple factors of authentication (MFA) is particularly useful for protecting your most sensitive services and applications. For example, you can force users to enter a login password and then enter a verification code that they receive by phone before accessing critical financial documents. To reduce the frequency of MFA challenges that interrupt the user workflow, you can specify an authentication timeout period during which a user responds to the challenges only once for repeated access to services and applications.

The MFA factors that the firewall supports include Push, Short Message Service (SMS), Voice, and One-time password (OTP) authentication. The firewall integrates with MFA vendors through:

- APIs—The supported vendors are Duo v2, Okta Adaptive, and PingID. Palo Alto Networks will periodically add or update support for MFA vendor APIs through Applications content updates.
- RADIUS—The firewall supports all vendors through RADIUS.

Configure Authentication Policy with MFA

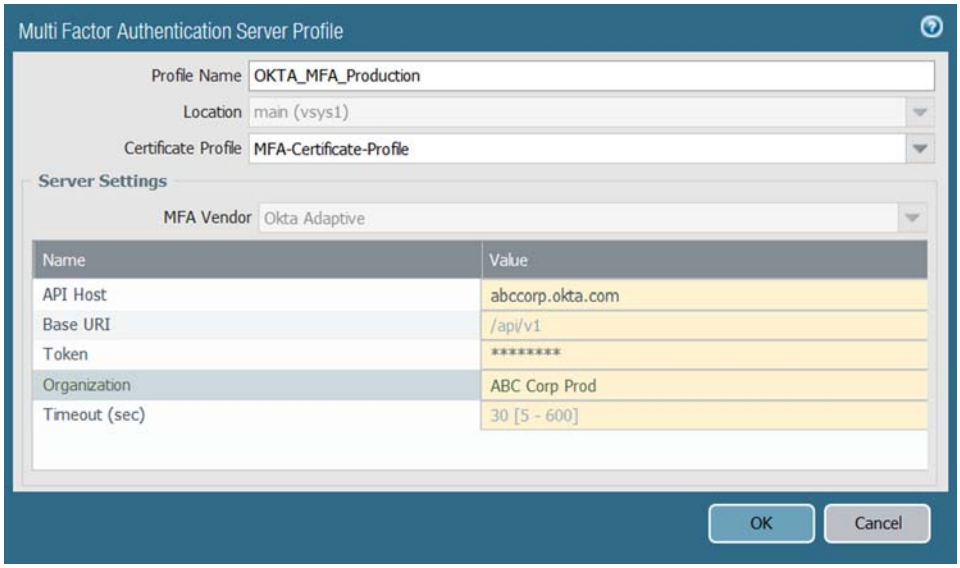
Step 1 Configure Captive Portal in **Redirect** mode.

The firewall uses the Captive Portal web form to prompt users for the first authentication factor. The firewall also uses Captive Portal to record the timestamps associated with successful authentication events. The firewall uses the timestamps to evaluate the authentication timeout periods that you set in Authentication policy rules (later in this procedure).

Step 2 Configure a server profile that defines how the firewall connects to the service that provides the first authentication factor.

For example, to add an LDAP server profile, select **Device > Server Profiles > LDAP** and **Add** a profile.

Step 3 Select **Device > Server Profiles > Multi Factor Authentication** and **Add** an MFA server profile for each authentication factor after the first factor.

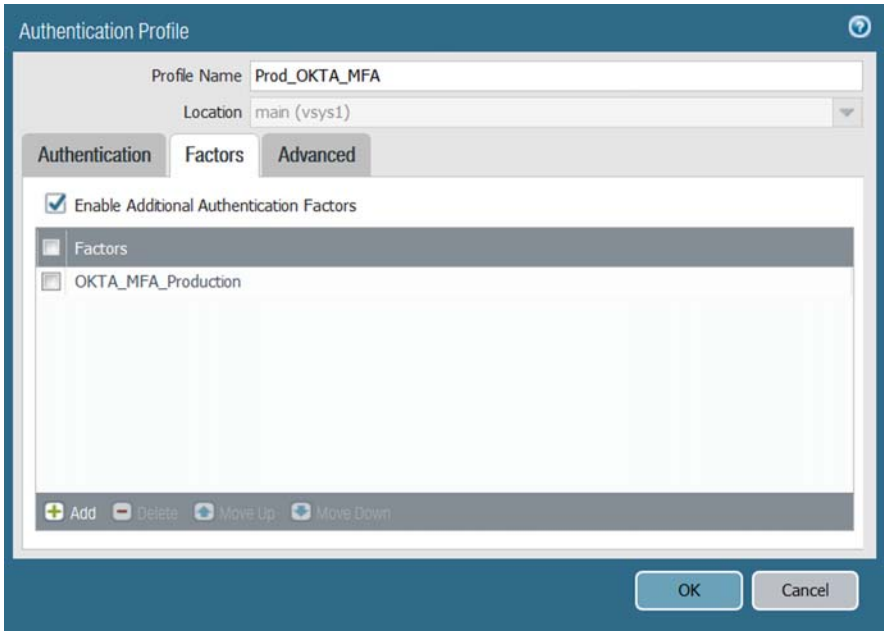


Configure Authentication Policy with MFA (Continued)

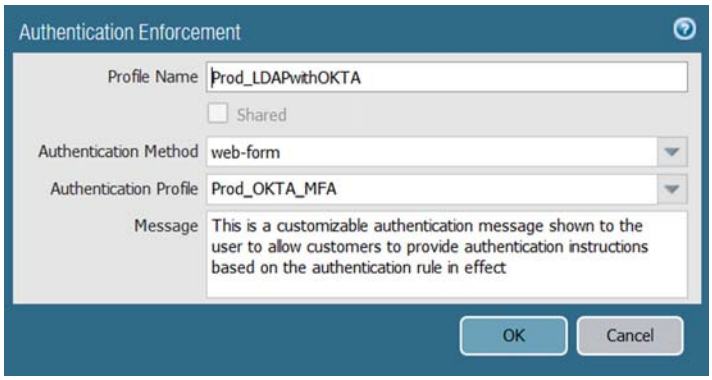
Step 4 Select **Device > Authentication Profile** and **Add** an authentication profile.

The profile specifies the order in which the firewall evokes authentication factors.

- First factor—Select the **Type** and select the **Server Profile** you configured.
- Additional factors—Select **Factors**, **Enable Additional Authentication Factors**, and **Add** the MFA server profiles you configured.



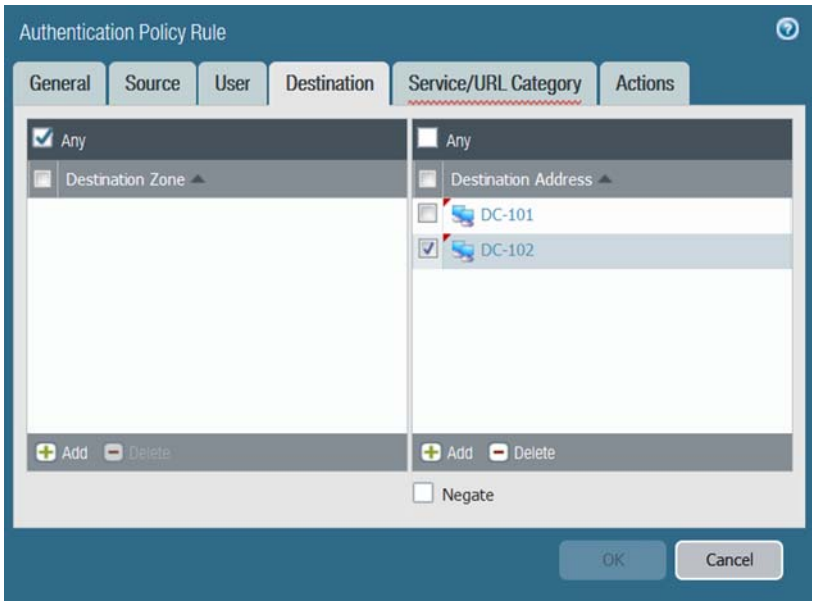
Step 5 Select **Objects > Authentication** and **Add** an authentication enforcement object to associate the authentication profile with a Captive Portal method for authenticating users and for recording authentication timestamps.



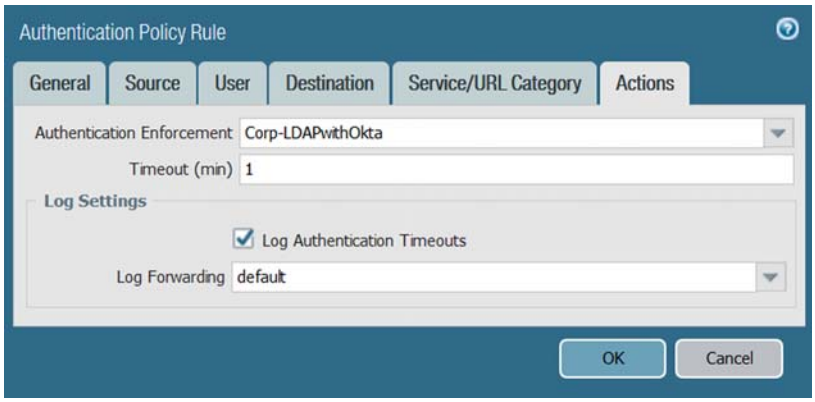
Configure Authentication Policy with MFA (Continued)

Step 6 Select **Policies > Authentication** and **Add** an Authentication policy rule.

- For the Destination Address, you can specify the IP addresses of the services and applications (such as servers) that require authentication for users to access them.



- For the **Actions**, select the **Authentication Enforcement** object you configured and specify the **Timeout** period in minutes (default 60) during which the firewall prompts the user to authenticate only once for repeated access to services and applications. The firewall evaluates the **Timeout** based on the timestamps it recorded for authentication events.



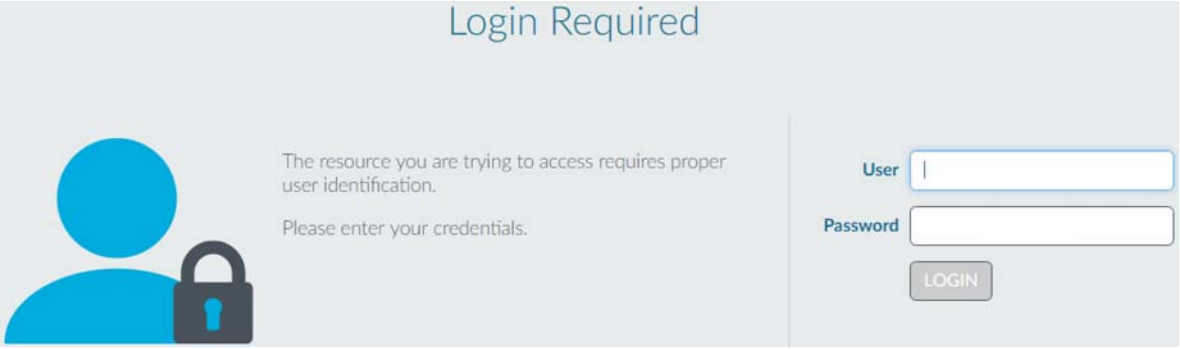
Step 7 Customize the MFA login page that the firewall displays to tell users how to respond to MFA challenges—Select **Device > Response Pages**, select **MFA Login Page**, **Export** the **Predefined** response page to your client system, and use an HTML editor to customize the page. When you finish customizing the page, save it with a unique name and **Import** it back onto the firewall.

Step 8 Configure a Security policy that allows users to access the services and applications that require authentication, and then **Commit** your changes.

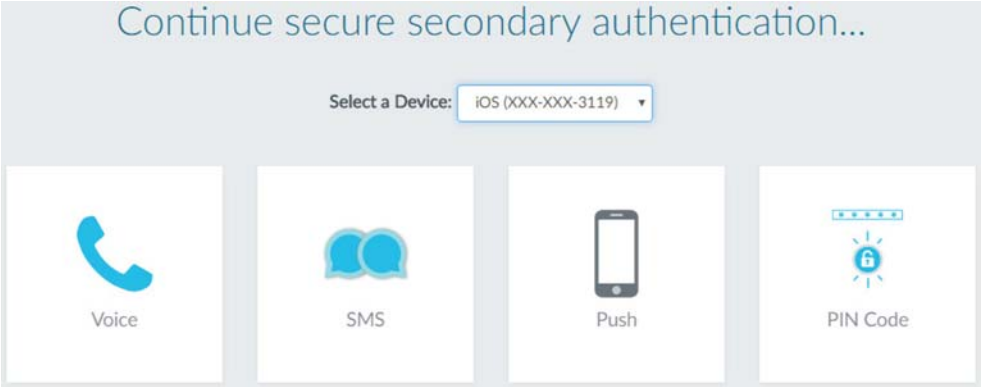
Configure Authentication Policy with MFA (Continued)

Step 9 Verify that the firewall enforces MFA by logging in to your network as one of the users specified in the Authentication rule and requesting a service or application specified in the rule.

The firewall displays the Captive Portal web form for the first authentication factor.



After you enter your login credentials, the firewall displays an MFA login page for the next authentication factor.



After you respond to all the authentication factors, the firewall evaluates Security policy and provides access to the service or application.

The automated correlation engine on the firewall uses several new correlation objects to detect events on your network that could indicate credential abuse relating to MFA. To review the events, select **Monitor > Automated Correlation Engine > Correlated Events**.

TACACS+ User Account Management

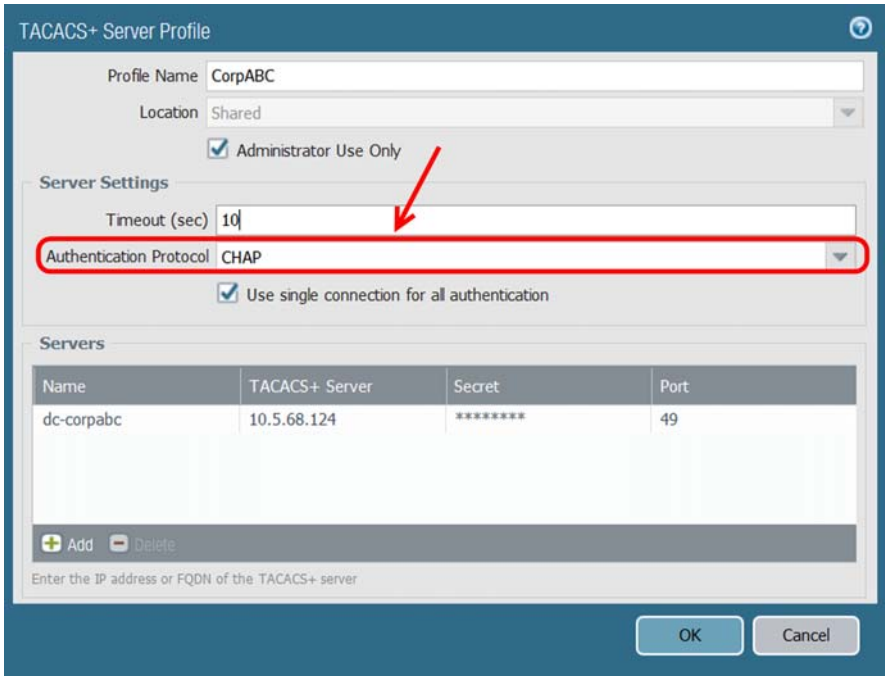
You can now use Terminal Access Controller Access-Control System Plus (TACACS+) Vendor-Specific Attributes (VSAs) to manage firewall and Panorama administrator accounts on an external server. Using an external server to centrally manage all administrators is useful in deployments where you don't want to use the firewall and Panorama to manage a subset of administrators. You can manage both authentication and authorization for administrators. For authorization, TACACS+ VSAs enable you to quickly change the roles, access domains, and user groups of administrators through your directory service instead of reconfiguring settings on the firewall and Panorama.

In this example procedure, you configure authentication and authorization for firewall administrator accounts that you manage on a TACACS+ server.

Configure TACACS+ Authentication and Authorization

Step 1 Select **Device > Server Profiles > TACACS+** and **Add** a TACACS+ server profile to define how the firewall connects to the server.

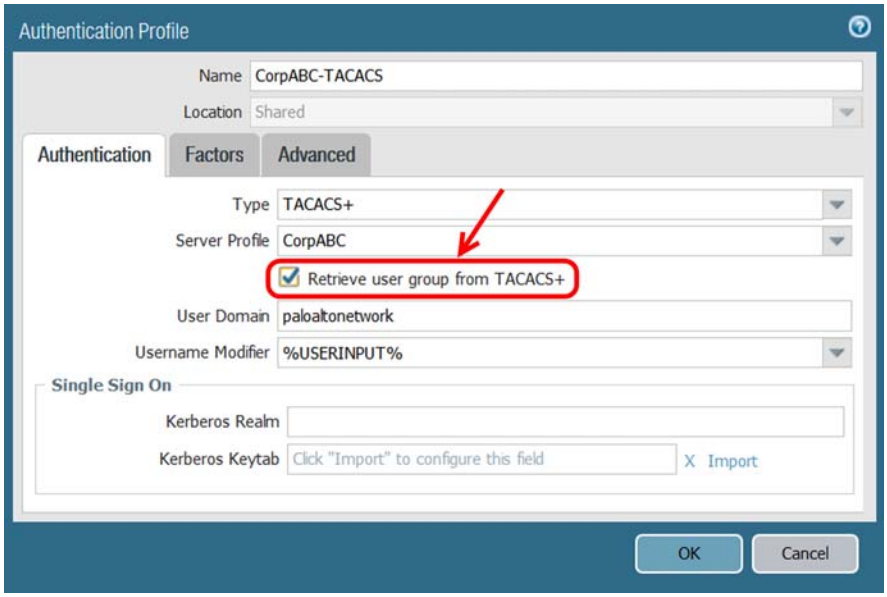
As a best practice, select **CHAP** if the TACACS+ server supports that **Authentication Protocol**; it is more secure than **PAP**.



Configure TACACS+ Authentication and Authorization (Continued)

Step 2 Select **Device > Authentication Profile** and **Add** an authentication profile to specify the server profile you configured and to configure authentication settings.

You must **Retrieve user group from TACACS+** to collect user group information from VSAs defined on the TACACS+ server. The firewall matches the group information against the groups you specify in the Allow List (**Advanced** settings) of the authentication profile.



Step 3 Enable the firewall to use the authentication profile for all administrators—Select **Device > Setup > Management**, edit the Authentication Settings, select the **Authentication Profile** you configured, and click **OK**.

Step 4 Configure an Admin Role profile if the administrator will use a custom role instead of a predefined (dynamic) role.

Step 5 Select **Device > Access Domain** and **Add** access domains if the firewall has more than one virtual system.

Step 6 **Commit** your changes.

Step 7 Configure the TACACS+ server—Refer to your TACACS+ server documentation for the steps to:

- Add the firewall IP address or hostname as the TACACS+ client.
- Add the administrator accounts.

If you selected **CHAP** as the **Authentication Protocol**, you must define accounts with reversibly encrypted passwords. Otherwise, CHAP authentication will fail.

- Define TACACS+ VSAs for the role, access domain, and user group of each administrator.

Step 8 Verify that the TACACS+ server performs authentication and authorization for administrators by logging in to the firewall web interface with an administrator account that you added to the TACACS+ server. Verify the following:

- You can access only the web interface pages that are allowed for the role you associated with the administrator.
- In the **Monitor**, **Policies**, and **Objects** tabs, you can access only the virtual systems that are allowed for the access domain you associated with the administrator.

Authentication Using Custom Certificates

You can now configure mutual authentication of Panorama, firewalls, and Log Collectors using custom certificates. This allows you to establish a unique chain of trust between Panorama and its managed devices instead of relying on predefined certificates used for management and inter-device communication. You can also configure custom certificates for mutual authentication between the Windows User-ID agent and the firewalls; this connection is used for sending user mapping information from the agent to the firewall. User-ID mapping information redistribution between firewalls and Panorama use the existing connections between Panorama and its managed devices. Additionally, you can use custom certificates for authentication between Panorama high availability (HA) peers. You can generate these certificates locally on Panorama or the firewall, obtain them from a trusted third-party certificate authority (CA), or obtain certificates from your own enterprise CA. By using custom certificates, you can establish a unique chain of trust to ensure mutual authentication between Panorama and the devices it manages.

Beginning in 8.0.1, you can also configure custom certificates for mutual authentication between the Terminal Services agent and the firewalls.

- Deploy Custom Certificates
- Deploy Custom Certificates for Panorama HA
- Deploy a Custom Certificate on Windows User-ID Agent
- Deploy a Custom Certificate on the Terminal Services Agent

Deploy Custom Certificates

Complete the following procedure to obtain custom certificates and deploy them on your Panorama and its managed devices.

Deploy Custom Certificates		
Step 1	Generate or obtain your server and client certificates.	Based in the needs of your organization, choose one of the supported methods for generating or obtaining your custom certificates.
Step 2	Configure the server certificate profile and SSL/TLS service profile for Panorama or server Log Collector.	1. Configure a certificate profile. This profile includes the server certificate, as well as the root and intermediate CAs. 2. Configure an SSL/TLS service profile.

Deploy Custom Certificates	
Step 3 Configure Secure Server Communication on Panorama or Log Collector.	1. Select the SSL/TLS service and certificate profiles for secure server communication. 2. Optionally, you can add another layer of security by authorizing clients. • You can configure an authorization list. The authorization list checks the client certificate Subject or Subject Alt Name. If the Subject or Subject Alt Name presented with the client certificate does not match an identifier on the authorization list, authentication is denied. • You can configure Panorama can also authorize firewalls and Log Collectors based on their serial number. 3. Do not check **Allow Custom Certificates Only** until you have deployed custom certificates on your managed devices. 4. Set the **Disconnect Wait Time in minutes**. This is the amount of time Panorama waits to terminate its current connection with managed devices before breaking that connection and reestablishing it using custom certificates for authentication. When you commit your configuration, the wait time count down begins.
Step 4 Configure the client certificate profile on the firewall or Panorama (and push it applicable managed devices).	Configure a certificate profile or profiles for the device or devices managed by Panorama. You can configure a unique certificate profile for each managed device or push the certificate profile to manged devices as part of a template. You can use a local certificate or obtain a certificate from a Simple Certificate Enrollment Protocol (SCEP) server.
Step 5 Deploy the client certificates on firewalls or Log Collectors.	1. On the firewall or client Log Collector, configure the **Secure Client Connection** settings. Assign the certificate or SCEP profile and certificate profile for the firewall to use for authentication. Additionally, the firewall can verify the server's identity by checking matching the server's IP address or FQDN with common name in the server certificate. 2. **Commit** your changes. After committing your changes, the firewall will begin using the custom certificate when the disconnect wait time is complete and the server has terminated its current connection to the client.
Step 6 Enforce the use of custom certificates.	1. Return to Panorama or the server Log Collector. By selecting, **Allow Customer Certificate Only**, all devices managed by Panorama must use custom certificates. If not, authentication between Panorama and the firewall or Log Collector fails. 2. To add additional managed devices, you must deploy the certificates on the firewall or Log Collector before adding it to Panorama or disable custom-certificate enforcement until the certificate is deployed.

Deploy Custom Certificates for Panorama HA

You can configure mutual authentication using custom certificates for securing the HA connection between Panorama HA peers. Complete the following procedure to obtain custom certificates and deploy them on your Panorama HA peers.

Deploy Custom Certificates for Panorama HA		
Step 1	Generate and deploy custom certificates on the primary Panorama.	1. Generate a certificate authority (CA) certificate on Panorama. 2. Configure a certificate profile that includes the root CA and intermediate CA. 3. Configure an SSL/TLS service profile.
Step 2	Configure Secure Server Communication on the primary Panorama.	1. Assign the SSL/TLS service and certificate profiles for secure server communication. 2. Do not check **Allow Custom Certificates Only** until you have deployed custom certificates on your managed devices. 3. Set the **Disconnect Wait Time** in minutes. This is the amount of time Panorama waits to terminate its current connection with managed devices before breaking that connection and reestablishing it using custom certificates for authentication. When you commit your configuration, the wait time count down begins.
Step 3	Configure the client certificate profile on the secondary Panorama.	Configure a certificate profile or profiles for the device or devices managed by Panorama.
Step 4	Configure Secure Client Communication on the secondary Panorama.	1. Configure the **Secure Client Connection** settings. Assign the certificate and certificate profile for the firewall to use for authentication. Additionally, the firewall can verify the server's identity by checking matching the server's IP address or FQDN with common name in the server certificate. 2. **Commit** your changes. After committing your changes, the firewall will begin using the custom certificate when the disconnect wait time is complete and the server has terminated its current connection to the client.
Step 5	Enforce the use of custom certificates.	After deploying client certificates on all managed devices, return to Panorama or the server Log Collector. By selecting, **Allow Customer Certificate Only**, all devices managed by Panorama must use custom certificates. If not, authentication between the Panorama peers fails.

Deploy a Custom Certificate on Windows User-ID Agent

Complete the following procedure to obtain and deploy custom certificates for mutual authentication between the Windows User-ID Agent and a firewall.

Deploy Custom Certificates on the Windows User-ID Agent		
Step 1	Generate or obtain your server and client certificates.	Based in the needs of your organization, choose one of the supported methods for generating or obtaining your custom certificates. The server certificate, installed on the Windows User-ID Agent, requires an encrypted private key and uploaded using the PFX or P12 bundles.
Step 2	Upload the server certificate to the Windows User-ID Agent.	Under **Server Certificate** on the Windows User-ID agent, upload the server certificate and enter the private key password.
Step 3	Configure the client certificate profile on the firewall.	Configure a certificate profile for the firewall.
Step 4	Apply the certificate profile.	On the firewall, select **Device > User Identification > Connection Security** and choose the certificate profile.

Deploy a Custom Certificate on the Terminal Services Agent

Beginning in 8.0.1, you can complete the following procedure to obtain and deploy custom certificates for mutual authentication between the Terminal Services Agent and a firewall.

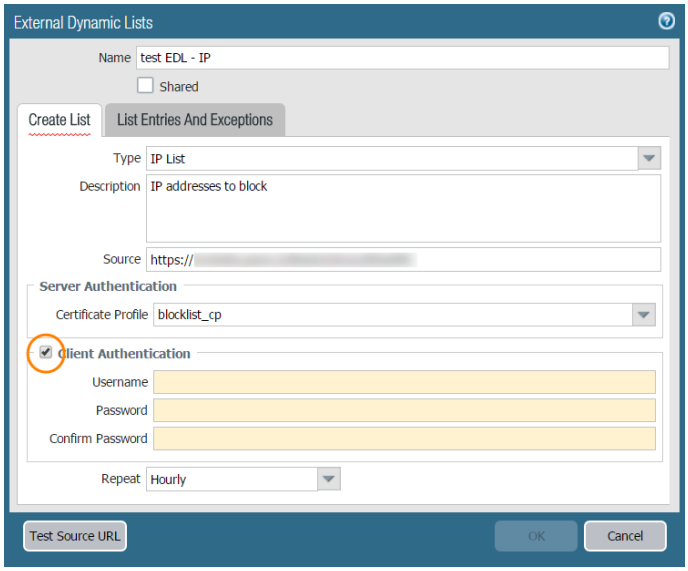
Deploy Custom Certificates on the Terminal Services Agent		
Step 1	Generate or obtain your server and client certificates.	Based in the needs of your organization, choose one of the supported methods for generating or obtaining your custom certificates. The server certificate, installed on the Terminal Services Agent, requires an encrypted private key.
Step 2	Upload the server certificate to the Terminal Services Agent.	Under **Server Certificate** on the Terminal Services agent, upload the server certificate and enter the private key password.
Step 3	Configure the client certificate profile on the firewall.	Configure a certificate profile for the firewall.
Step 4	Apply the certificate profile.	On the firewall, select **Device > User Identification > Connection Security** and choose the certificate profile.

Authentication for External Dynamic Lists

When retrieving external dynamic lists hosted on SSL/TLS secured servers (servers with an HTTPS URL), the firewall now validates the digital certificates of the server before proceeding with the retrieval. You must now enable server authentication for these external dynamic lists for the firewall to retrieve them. Additionally, you can now retrieve external dynamic lists hosted on SSL/TLS secured servers that enforce basic HTTP username/password authentication (client authentication). Server authentication prevents man-in-the-middle attacks by ensuring that the firewall retrieves an external dynamic list from a valid source, not a malicious or spoofed server, while client authentication allows you to use more secure sources (such as MineMeld) that limit access to their external dynamic lists to authorized users. If the certificate of an external dynamic list server is expired or revoked, or if you enter incorrect login credentials for the list, authentication fails. The firewall then ceases to enforce policy based on the list contents.

In Panorama, you can use external dynamic lists to enforce policy across multiple firewalls in a device group. Panorama enforces policy without server and client authentication for firewalls running PAN-OS 7.1 and earlier versions.

Enable Authentication for an External Dynamic List		
Step 1	Select **Objects > External Dynamic Lists**, and click on a dynamic IP, domain, or URL list.	
Step 2	(New) If the server hosting the external dynamic list is secured with SSL (i.e., lists with an HTTPS URL), enable server authentication. You cannot edit or save changes to an external dynamic list with an HTTPS URL if you don't enable server authentication first.	Select an existing **Certificate Profile** for the list, or create a **New Certificate Profile**. A certificate profile authenticates a device and its certificates. The certificate profile you select must have a root CA certificate that matches the certificate installed on the server you are authenticating (also an intermediate CA certificate, if the server has one). It is also recommended that you enable CRL and/or OCSP status verification, which checks the revocation status of the server certificates. Learn more about how to configure a certificate profile. If the external dynamic list source has an HTTP URL, you are not required to select a certificate profile. The firewall connects to the server that hosts the external dynamic list without certificate validation.  Maximize the number of external dynamic lists that you can use to enforce policy. Use the same certificate profile to authenticate external dynamic lists from the same source URL. If you assign different certificate profiles to external dynamic lists from the same source URL, the firewall counts each list as a unique external dynamic list.

Enable Authentication for an External Dynamic List (Continued)		
Step 3	(New) If the source of the external dynamic list has an HTTPS URL and requires a username and password for list access, enable client authentication.	1. Select **Client Authentication**.  2. Enter the username and password required by the list source. 3. Re-enter the password to confirm it.
Step 4	(Optional) Test the connectivity of the firewall to the server hosting the external dynamic list.	Click **Test Source URL**. A popup indicates whether the server is accessible. The **Test Source URL** button only verifies that the firewall can connect to the server. It does not check the status of the server's certificate.
Step 5	Save the configuration.	Click **OK** and **Commit**.
Step 6	Find external dynamic lists that failed authentication.	External dynamic lists that fail server or client authentication require your immediate attention because the firewall ceases to enforce policy based on their contents. The firewall generates critical system logs to alert you of authentication failure. To manually check if an external dynamic list authenticates successfully, retrieve an external dynamic list from the web server. If a server fails to authenticate, you can disable server authentication as a stop-gap measure until the owner of the external dynamic list addresses the cause of the failure.

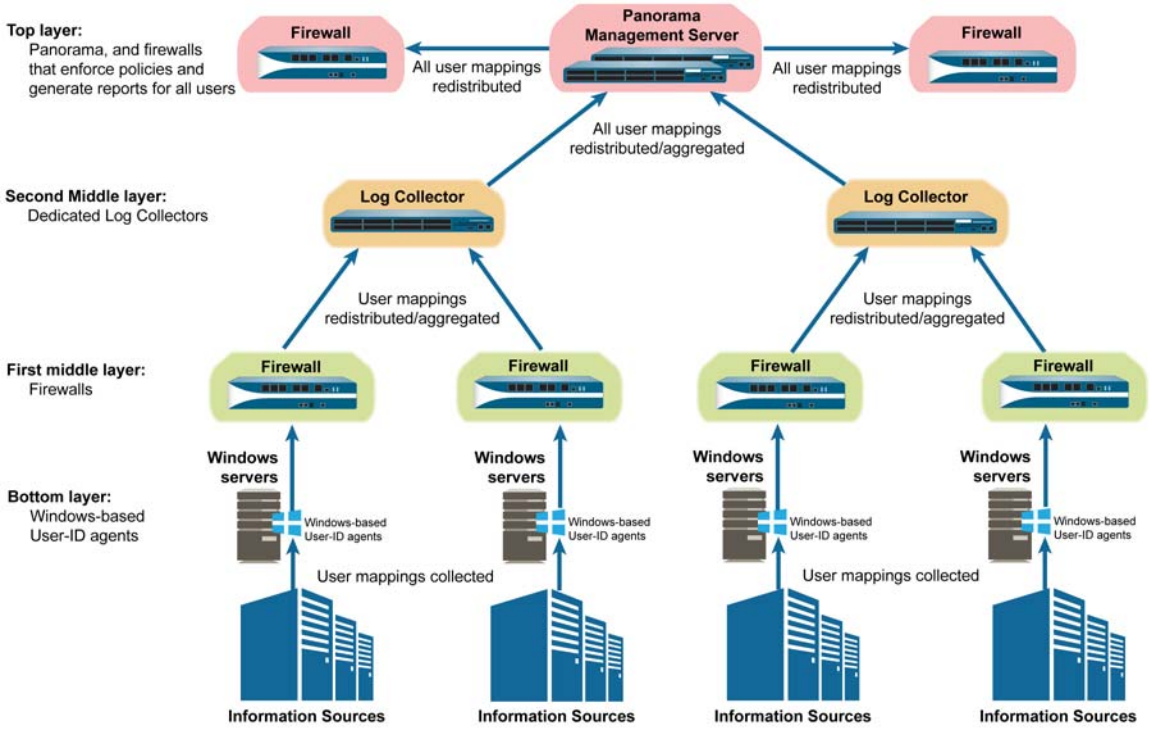
User-ID Features

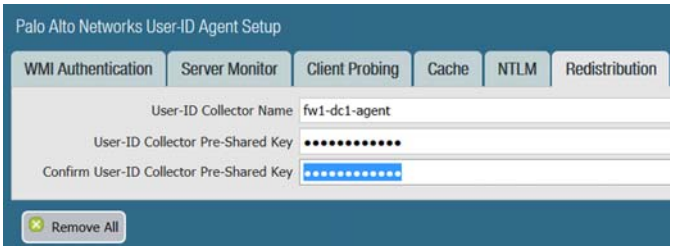
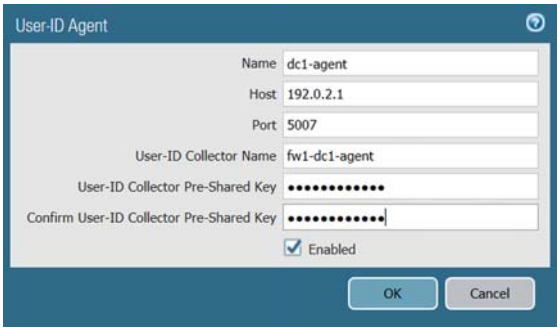
Panorama and Log Collectors as User-ID Redistribution Points

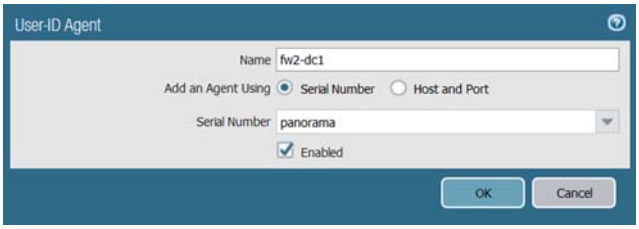
You can now leverage your Panorama and distributed log collection infrastructure to redistribute User-ID mappings in large-scale deployments. Because the infrastructure will have existing connections from firewalls to Log Collectors to Panorama, you can aggregate the mappings on Panorama without the administrative hassle of setting up extra connections between firewalls. Panorama can then redistribute the aggregated mappings to the firewalls that you use to enforce policies and generate reports for all the users in your network. Each Panorama management server, Log Collector, and firewall can receive user mappings from up to 100 redistribution points. The redistribution points can be Windows-based User-ID agents or other Panorama management servers, Log Collectors, and firewalls.

You cannot redistribute group mapping information or redistribute user mapping information collected from Terminal Services (TS) agents.

Figure: Panorama and Log Collectors as User-ID Redistribution Points



Configure Panorama and Log Collectors as User-ID Redistribution Points		
Step 1	Configure the firewalls to redistribute mapping information. In this example procedure, you use Panorama to push configurations to the firewalls. Therefore, the firewalls must be managed devices.	1. Log in to the Panorama web interface. 2. Configure the firewalls to function as User-ID redistribution points—Select **Device > User Identification > User Mapping**, select the **Template** to which the firewalls are assigned, edit the Palo Alto Networks User-ID Agent Setup, and configure the **Redistribution** settings.  3. Enable User-ID traffic on an interface that the firewall uses when responding to User-ID mapping queries from receiving devices (Log Collectors, in this example). You can use Panorama templates to perform this task for multiple firewalls.
Step 2	Configure each Log Collector to receive mapping information from firewalls and to redistribute the information to Panorama.	1. Add the firewalls as redistribution points to the Log Collector—Select **Panorama > Managed Collectors**, edit the Log Collector, select **User-ID Agents**, and **Add** each firewall.  2. Enable the management (MGT) interface of the Log Collector to respond to User-ID mapping queries from Panorama—Select **Interfaces**, click **Management**, select **User-ID** in the Network Connectivity Services section, and click **OK** twice.

Configure Panorama and Log Collectors as User-ID Redistribution Points (Continued)	
Step 3 Configure the Panorama management server to receive mapping information from Log Collectors and to redistribute the information.	1. Add the Log Collectors as User-ID redistribution points to Panorama—Select **Panorama > User Identification** and **Add** each Log Collector. Ignore the **Collector Name** and **Collector Pre-Shared Key** fields; they apply only when the User-ID agent is a firewall, not a Log Collector. 2. Enable the Panorama MGT interface to respond to User-ID mapping queries from the firewalls that enforce policies and generate reports—Select **Panorama > Setup > Interfaces**, click **Management**, select **User-ID** in the Network Connectivity Services section, and click **OK**.
Step 4 Configure the firewalls that enforce policies and generate reports to receive mapping information from Panorama.	1. Select **Device > User Identification > User-ID Agents**, select the **Template** to which the firewalls are assigned, and **Add** Panorama as a User-ID redistribution point.  2. Select **Commit > Commit and Push** to activate your changes on Panorama, the Log Collectors, and the firewalls.

Step 5 Verify that firewalls receive the redistributed mapping information.
This step samples a single user mapping redistributed to a single firewall. Repeat the step for several user mappings and several firewalls to ensure your configuration is successful.
	1. Access the CLI of a firewall that receives mappings from Windows-based User-ID agents or that uses its PAN-OS integrated User-ID agent to map IP addresses to usernames.
	2. Display all the user mappings on the firewall by running the following command:
	`> show user ip-user-mapping all`
	3. Record the IP address associated with any one username.
	4. Access the CLI of a top-layer firewall and run the following command, using the `<IP-address>` you recorded in the previous step:
	`> show user ip-user-mapping ip <IP-address>`
	If the firewall successfully received the user mapping, it displays output similar to the following, with the same username as you recorded in the middle-layer firewall.
	`IP address: 192.0.2.0 (vsys1)`
	`User: corpdomain\username1`
	`From: UIA`
	`Idle Timeout: 10229s`
	`Max. TTL: 10229s`
	`MFA Timestamp: first(1) - 2016/12/09 08:35:04`
	`Group(s): corpdomain\groupname(621)`

Centralized Deployment and Management of User-ID and TS Agents

You can now use endpoint management software such as Microsoft Windows Server Update Services (WSUS) to remotely install, configure, and upgrade multiple Windows-based User-ID agents and Terminal Services (TS) agents. Using endpoint management software streamlines your workflow by enabling you to deploy and configure numerous User-ID and TS agents in a single operation instead of using a manual login session for each agent.

User Groups Capacity Increase

You can now configure policies to reference more user groups. This is useful in environments where access control for each application or service is based on membership in a user group, and where the number of applications, services, and groups is increasing.

The number of distinct user groups that each firewall or Panorama can reference across all policies varies by model:

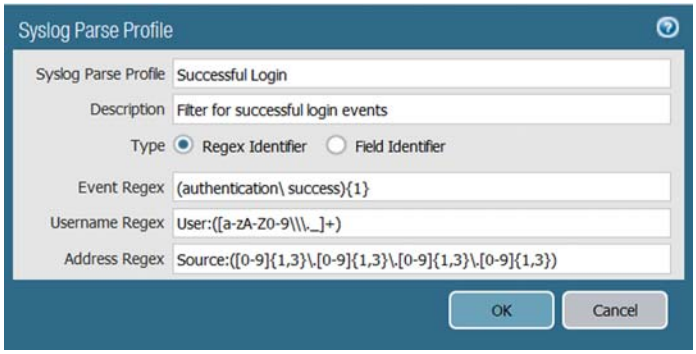
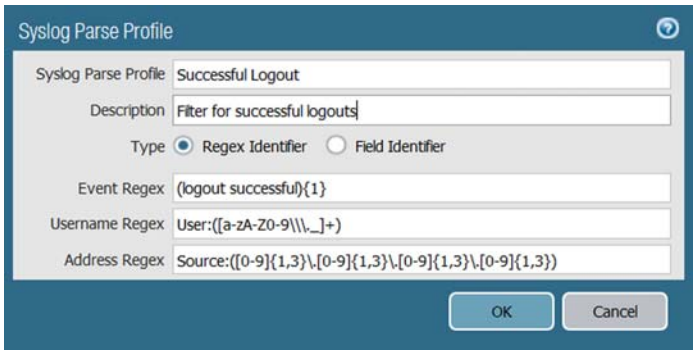
- VM-50, VM-100, VM-300, PA-200, PA-220, PA-500, PA-800 Series, PA-3020, and PA-3050 firewalls—1,000 groups
- VM-500, VM-700, PA-5020, PA-5050, PA-5060, PA-5200 Series, and PA-7000 Series firewalls, and all Panorama models—10,000 groups

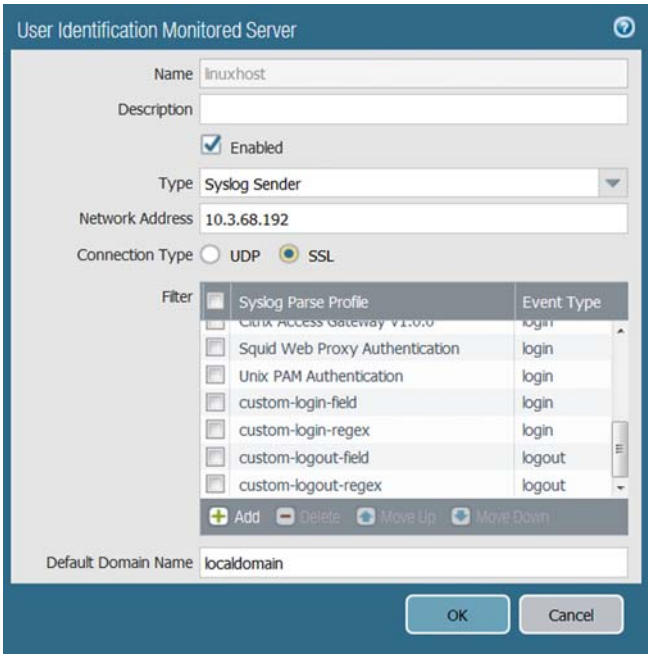
In this release, you will also find that error alerts for group mapping configurations are improved: the validation process now checks for errors in nested group lists. Nesting in this context describes group lists where individual list entries can also be group lists. The firewall and Panorama can validate group lists that are nested up to ten layers deep.

User-ID Syslog Monitoring Enhancements

The following enhancements improve the accuracy of User-ID mappings and simplify monitoring syslog senders for mapping information:

- Automatic deletion of user mappings—To improve the accuracy of your user-based policies and reports, you can now use syslog monitoring to detect when users have logged out; the firewall automatically deletes the associated User-ID mappings. Deleting outdated mappings is particularly useful in environments where IP address assignments change often.
- Multiple syslog formats—In environments where multiple points of authentication send syslog messages in different formats, it is now easier to collect user mappings from the messages because the firewall can ingest multiple syslog formats from the same syslog sender.

Collect and Delete User Mappings Through Monitoring Syslog Senders	
Step 1 Define custom Syslog Parse profiles so that the firewall filters syslog messages for login and logout events.	Select **Device > User Identification > User Mapping**, edit the Palo Alto Networks User-ID Agent Setup, select **Syslog Filters**, and **Add** a Syslog Parse profile. Each profile identifies either login events or logout events, but no single profile can identify both: • Example of Syslog Parse profile for login events:  • Example of Syslog Parse profile for logout events: 

Collect and Delete User Mappings Through Monitoring Syslog Senders (Continued)	
Step 2 Define the syslog senders that the firewall will monitor for syslog messages.	Select **Device > User Identification > User Mapping** and **Add** syslog senders to the Server Monitoring section. For syslog senders that send messages in multiple formats, **Add** a Syslog Parse profile for each format. Specify the event type (**login** or **logout**) for each profile. As a security best practice, select **SSL** when using the PAN-OS integrated User-ID agent to collect user mappings. 
Step 3 Enable syslog listener services in the Interface Management profile associated with the firewall interface used for user mapping.	Select **User-ID Syslog Listener-SSL** and/or **User-ID Syslog Listener-UDP** based on the connection types you specified for the syslog senders in the previous step.

Step 4 Commit and verify your changes.	1. **Commit** your changes.
	2. Log in to a client system for which a monitored syslog sender generates login and logout event messages.
	3. Log in to the firewall CLI.
	4. Verify that the firewall mapped the login username to the client IP address:
	`> show user ip-user-mapping ip <ip-address>`
	`IP address: 192.0.2.1 (vsys1)`
	`User: localdomain\username`
	`From: SYSLOG`
	5. Log out of the client system.
	6. Verify that the firewall deleted the user mapping:
	`> show user ip-user-mapping ip <ip-address>`
	`No matched record`

Group-Based Reporting in Panorama

Panorama now provides visibility into the activities of user groups in your network through the User Activity report, SaaS Application Usage report, custom reports, and the ACC. Panorama aggregates group activity information from all the firewalls that it manages. This enables you to filter logs and generate reports for groups across your entire network instead of just the groups that individual firewalls monitor. Analyzing group activity helps you understand resource usage and security risks in your network so that you can refine the policies that control access to those resources.

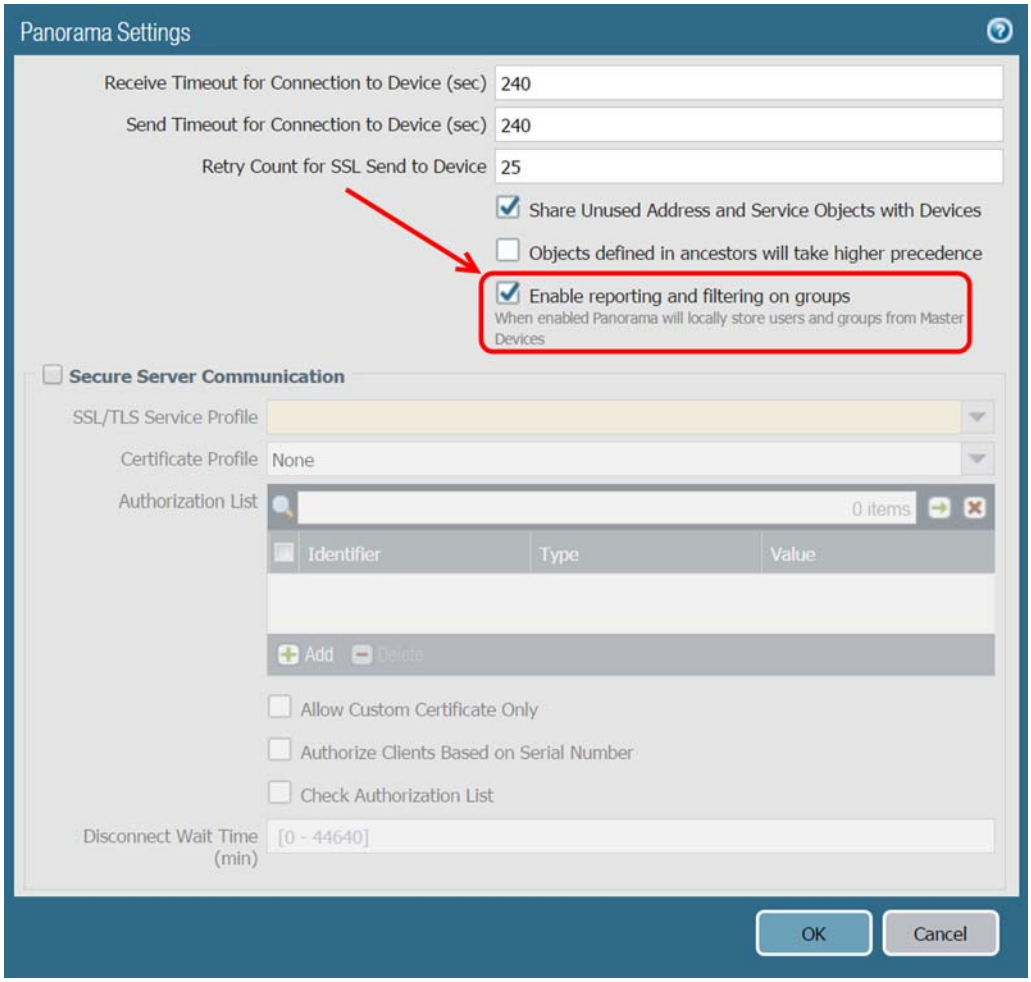
To enable Panorama to collect user group information, you must upgrade your managed firewalls to PAN-OS 8.0. Panorama cannot collect group information from firewalls running earlier PAN-OS releases.

- Filter Logs by Group on Panorama
- Configure a Group Activity Report on Panorama

Filter Logs by Group on Panorama

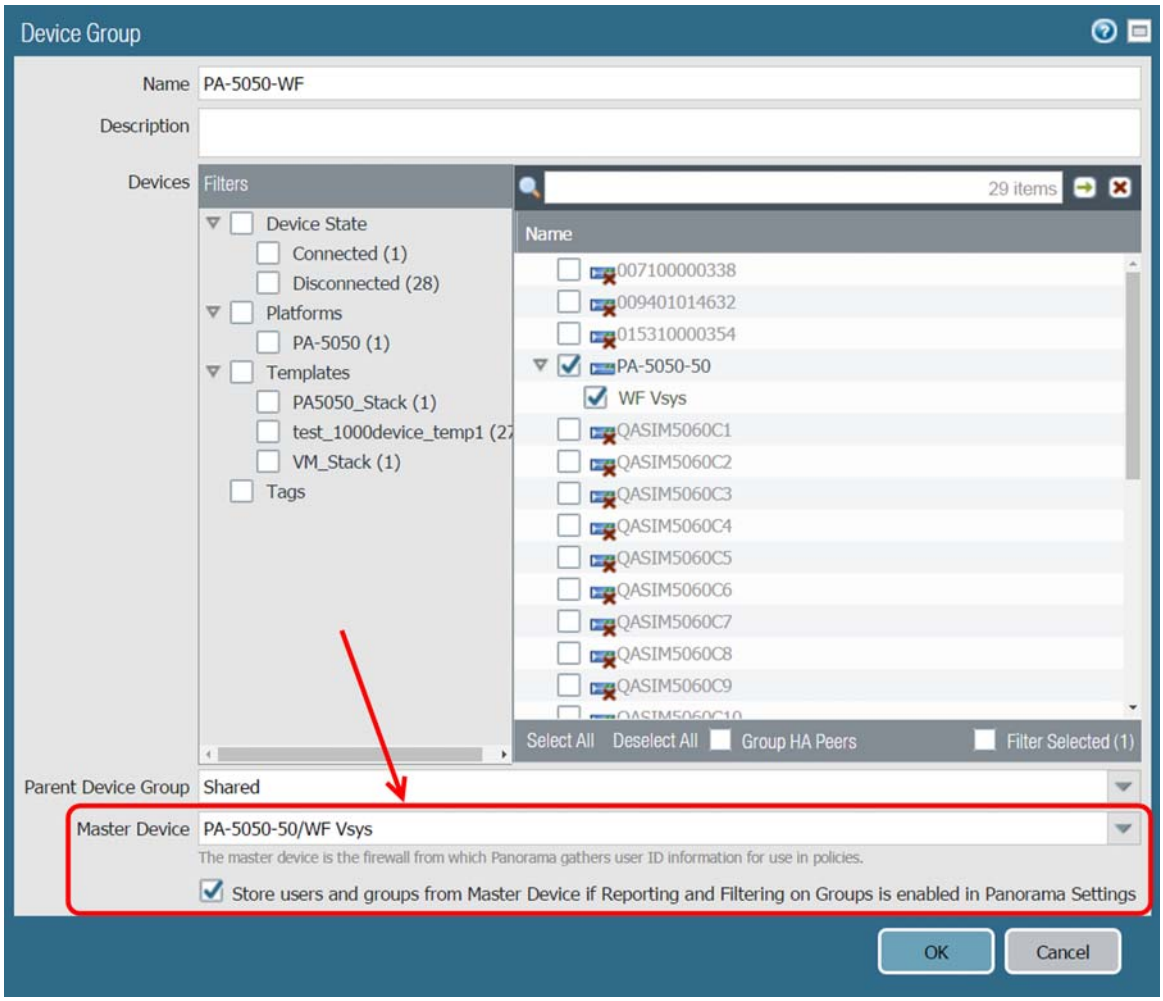
Filter Logs by Group on Panorama

Step 1 Select **Panorama > Setup > Management**, edit the Panorama Settings, and **Enable reporting and filtering on groups** so that Panorama can locally store user and user group information that it receives from firewalls.



Filter Logs by Group on Panorama (Continued)

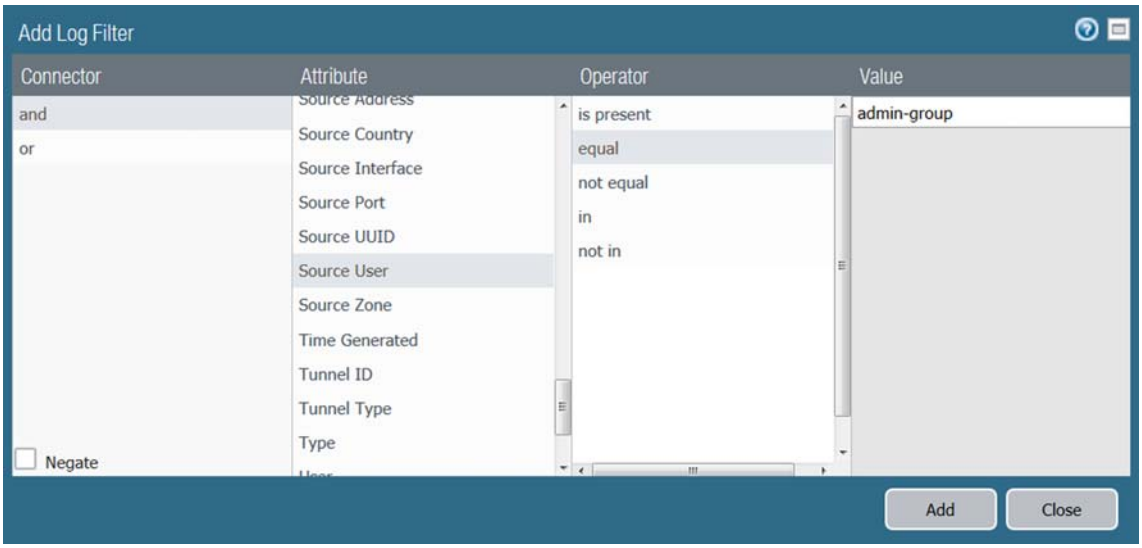
Step 2 Configure device groups so that Panorama can receive user group information from one **Master Device** (firewall) in each device group. You must enable Panorama to **Store users and groups from Master Device**.



Filter Logs by Group on Panorama (Continued)

Step 3 Filter logs by user group.

For example, to filter the Traffic logs, select **Monitor > Logs > Traffic** and Add Filter ( ). When you configure the query, set the Attribute to **Source User** and set the Value to the name of the user group.



After you Apply Filter ( ), the page displays logs only for traffic that users in the specified groups initiated.

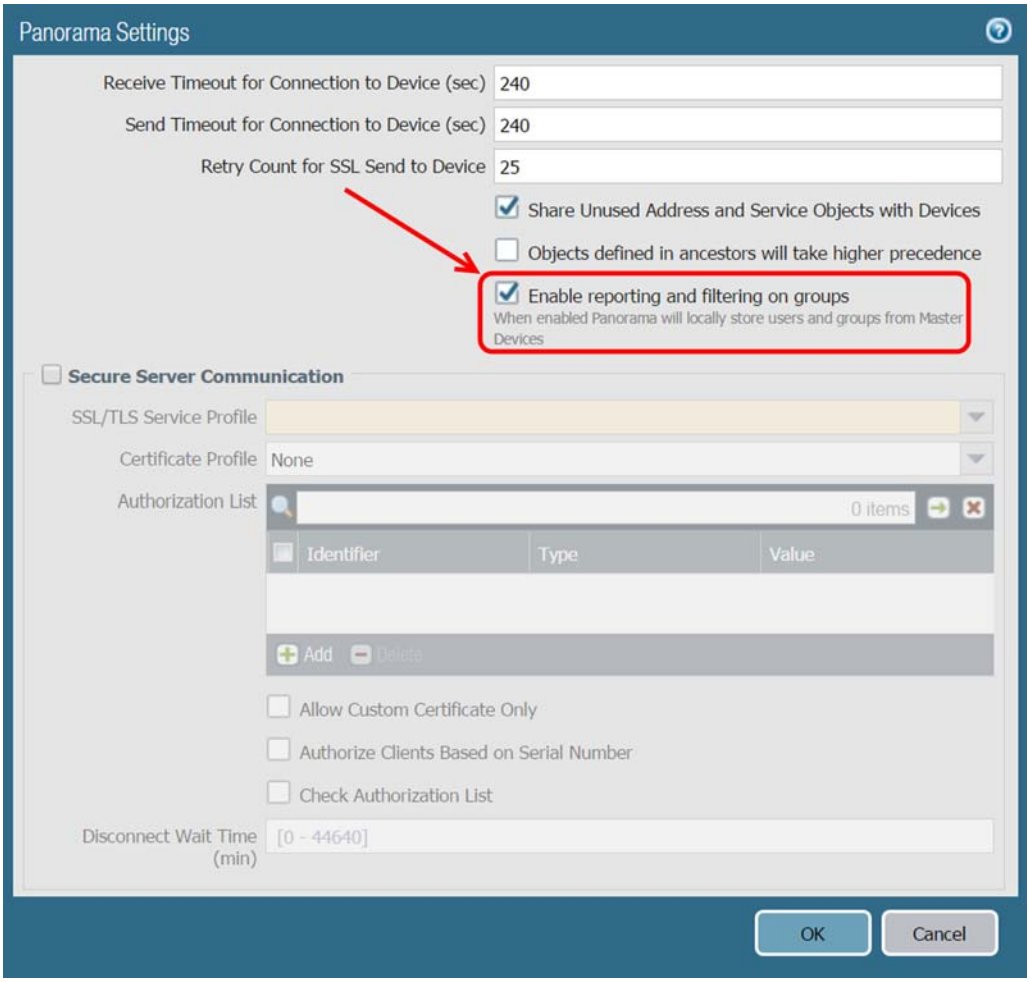
Configure a Group Activity Report on Panorama

Perform the following steps to generate a Group Activity report on Panorama. Group Activity reports summarize the web activities of user groups in your network.

You can also see group activity in a SaaS Application Usage report, custom report, or Application Command Center (ACC).

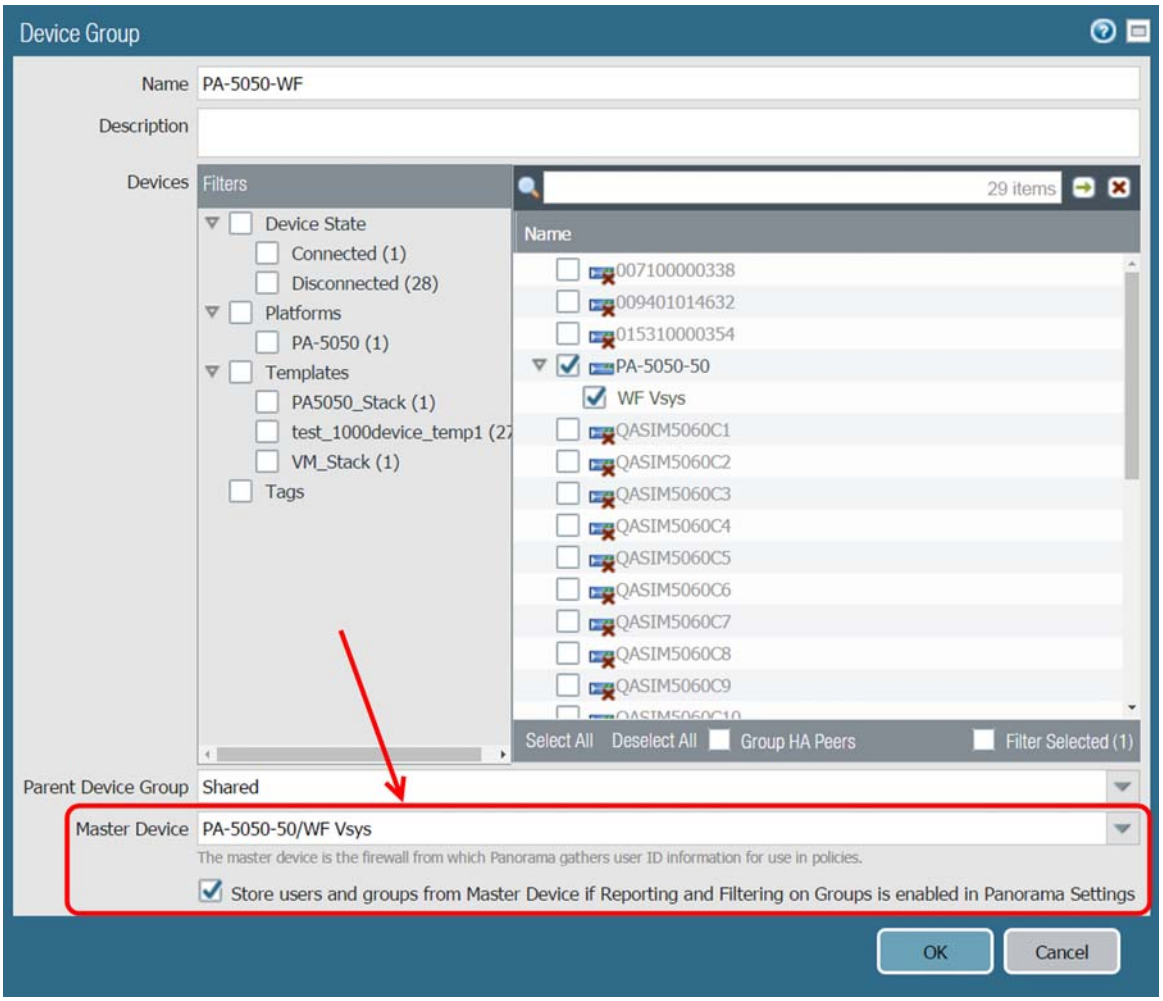
Generate a Group Activity Report on Panorama

Step 1 Select **Panorama > Setup > Management**, edit the Panorama Settings, and **Enable reporting and filtering on groups** so that Panorama can locally store user and user group information that it receives from firewalls.



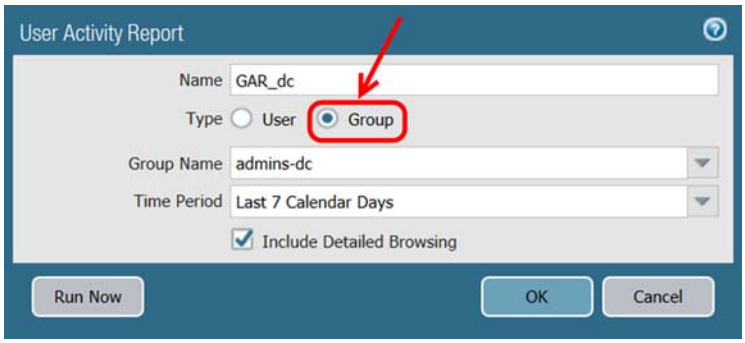
Generate a Group Activity Report on Panorama (Continued)

Step 2 Configure device groups so that Panorama can receive user group information from one **Master Device** (firewall) in each device group. You must enable Panorama to **Store users and groups from Master Device**.



Generate a Group Activity Report on Panorama (Continued)

Step 3 Select **Monitor > PDF Reports > User Activity Report**, **Add** a Group Activity report, set the **Type** to **Group**, select a **Group Name**, and specify the **Time Period** for the report.



You can generate the report:

- **Immediately**—**Run Now** and download the report.
- **At the same time as other saved reports**—Click **OK**, select **Commit > Commit to Panorama**, and **Commit** your changes.

App-ID Features

SaaS Application Visibility for User Groups

For better visibility in to SaaS activity on your network, PAN-OS 8.0 includes enhancements to the SaaS Application Usage report. In addition, the ACC and custom reports now help you identify, manage, and control risky SaaS application usage on your network.

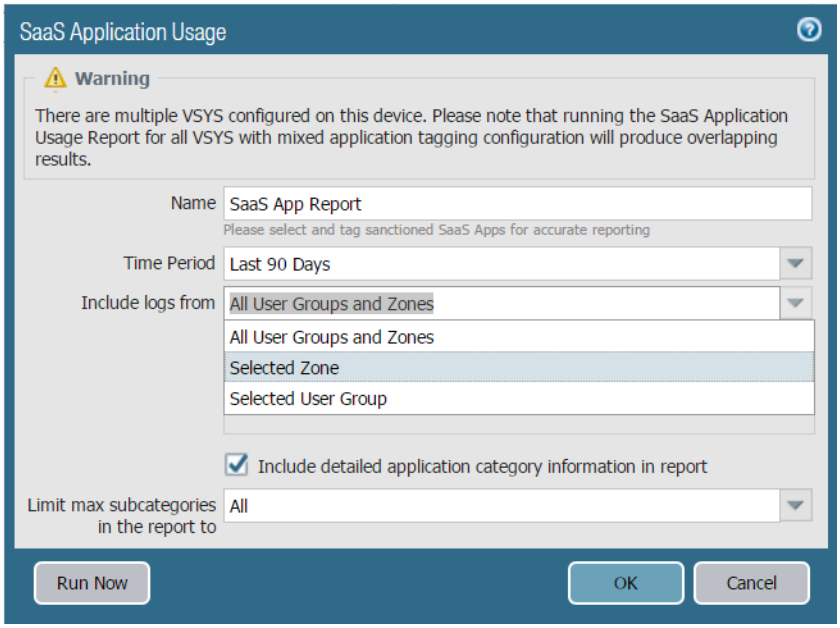
View a short video on these enhancements.

- SaaS Application Usage PDF report that was introduced in PAN-OS 7.1, is enhanced to highlight application usage by groups of users (departments). You can generate the report to view activity for user groups across all security zones on the firewall or Panorama, monitor activity for specific user group(s), or report on SaaS activity for a user group(s) within a specific zone. The first part of the 10-page PDF report (formerly 8-page report) includes two new pages that showcase the top user groups that use the largest number of SaaS applications, and the top user groups that transfer the largest volume of data through sanctioned and unsanctioned SaaS applications.

  And, you can now generate a custom report that depicts the number of SaaS applications used on your network and the unique user count by application. The unique user count is a new column in the report and the SaaS application characteristic (is SaaS) is a filter in the query builder.

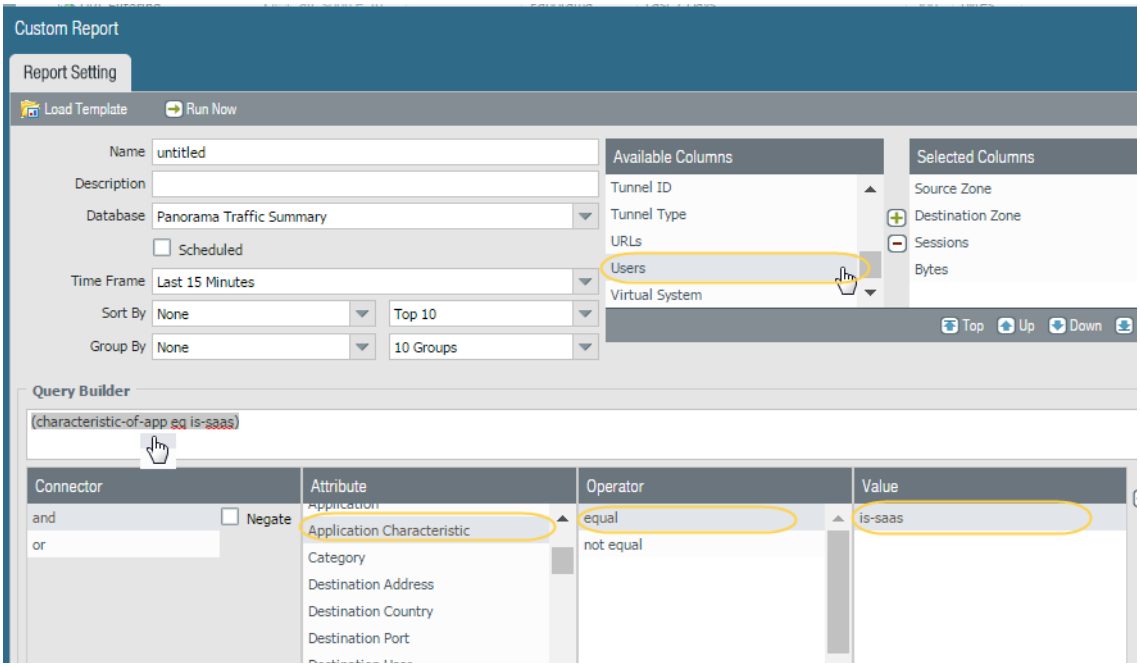
SaaS Application Usage Report and Custom Report Enhancements

- Generate the SaaS Application Usage report for a specific security zone or user group(s).



SaaS Application Usage Report and Custom Report Enhancements (Continued)

- Create a custom report to view the number of unique users who use SaaS applications (or a specific application such as Box) on your network.
  1. Select **Monitor > Manage Custom Reports**, and click **Add**.
  2. To view the number of unique users who use SaaS applications on your network, select Users from the Available Column and add it to the Selected Column. Then, use the query builder to add the application characteristic equals *is saas*., as shown below:

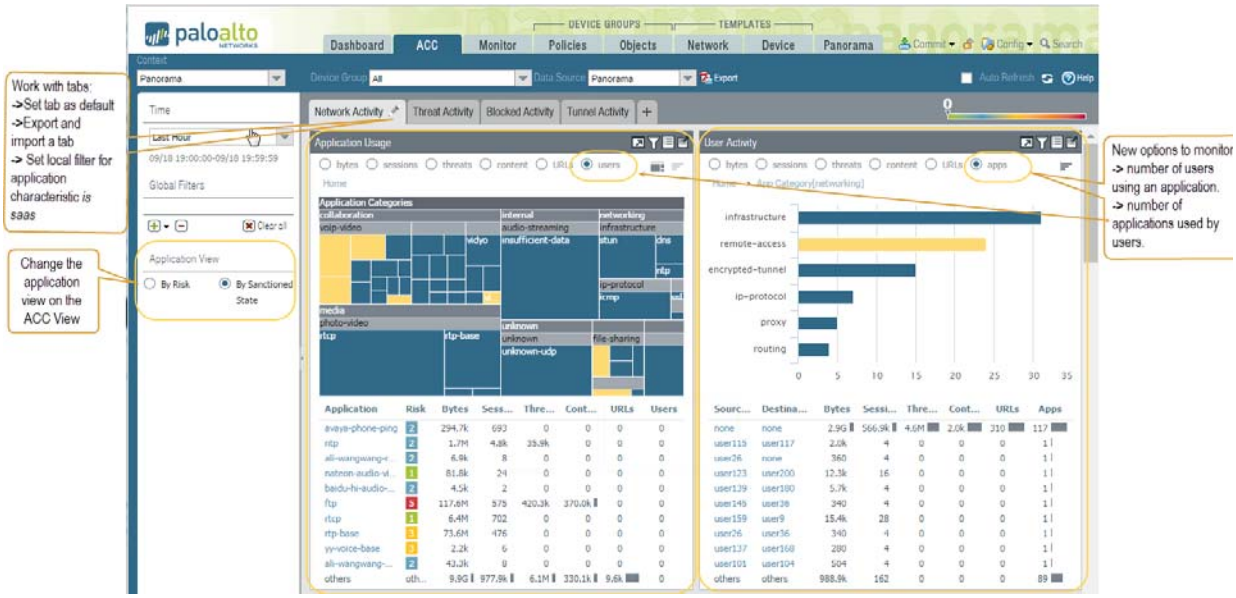


- **ACC Enhancements for SaaS Application Visibility**—The ACC has a new global filter to assess application activity on your network by risk and sanctioned state. When you apply the filter, all the ACC tabs pivot on risk state or sanctioned state so that you can determine the relative security risks associated with the SaaS applications traversing your network. You can also set any tab as the default tab so that the ACC layout retains your filter preferences, the next time you log in; export the tab, with your widget and local filters, and share it with another firewall administrator.

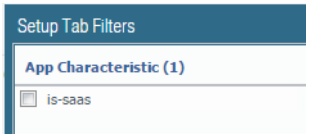
  If, for example, you want all your firewall administrators to use the Network Activity tab as the default tab with the application usage widget filtered on user count and the user activity widget filtered on application usage. You can export and share the tab with the other firewall administrators so that they can all consistently monitor for risk exposure on your network.

SaaS Visibility Enhancements in the ACC

- View the new colors in the Application Usage widget (**ACC >Network Activity)**.
  Sanctioned applications are depicted in green, and unsanctioned applications are blue. Applications that are not consistently tagged as sanctioned or unsanctioned across all device groups or virtual systems are yellow.



- Use the **Application View** global filter to view applications by risk or by sanctioned state.
- View the changes in the **ACC > Network Activity** tab:
  - Filter by user count in the Application Usage widget.
  - Filter by application count in the User Activity widget.
- Work with the ACC tabs. Click the edit icon in a tab to:
  - Set a tab as default.
  - Set a filter for Saas applications.



  - Export a tab.
    You can share the tab as a .txt file with another administrator.
  - Import a tab.
    Select the + icon along the list of tabs, and add a name and click the import icon, browse to select the .txt file.

Decryption Features

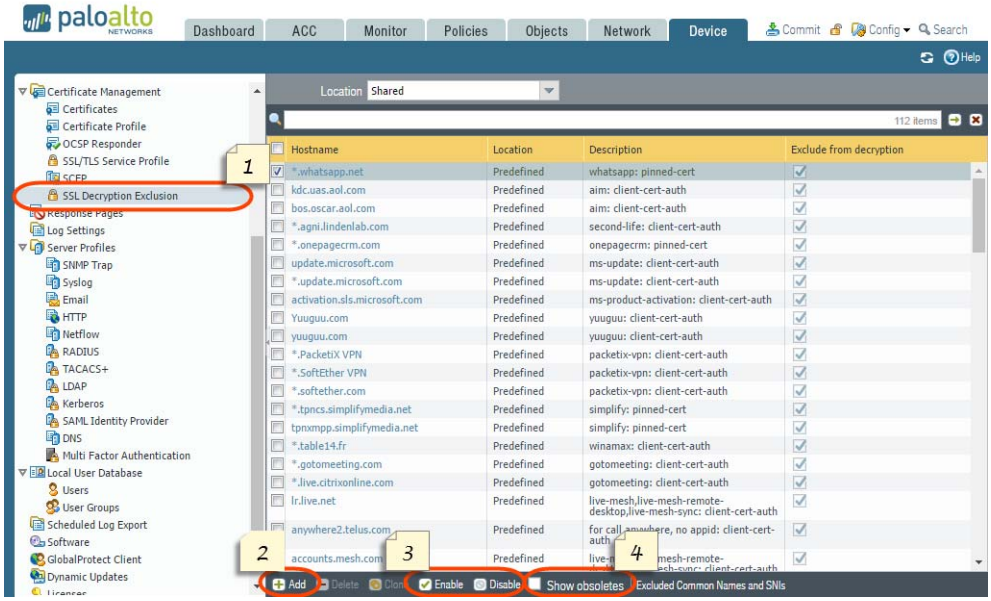
- Management for Certificates Excluded from Decryption
- Perfect Forward Secrecy (PFS) for Inbound SSL Sessions

Management for Certificates Excluded from Decryption

You now have increased flexibility and control to manage traffic excluded from decryption. Centralized management for decryption exclusions allows you to:

- View the applications and services that the firewall does not decrypt. Palo Alto Networks provides predefined decryption exclusions to indicate applications and services that do not function correctly when the firewall decrypts them. The Applications and Threats content update (or the Applications content update, if you do not have a Threat Prevention license) include updates and additions to predefined decryption exclusions.
- Exclude a server from decryption based on the server hostname. All traffic originating from or destined to that server is excluded from decryption. Certificates enabled as SSL exclude certificates in PAN-OS 7.1, where a targeted server was excluded from decryption based on the CN in the server certificate, are automatically recreated as custom decryption exclusions in PAN-OS 8.0.

Go over the following steps to create a decryption exclusion and to view both custom and predefined exclusions.



View and Manage Decryption Exclusions	
Step 1 View decryption exclusions.	Select **Device > Certificate Management > SSL Decryption Exclusions** and view the list of both predefined and custom decryption exclusions. Entry details show whether the exclusion is predefined or custom, provides a description of the exclusion, and indicates if the exclusion is enabled: • Location—Indicates that an entry is predefined, or, for custom entries, indicates whether the entry is shared across all virtual systems or if it's specific to a single virtual system. • Exclude from decryption—A selected checkbox indicates that the firewall is actively enforcing the decryption exclusion.

View and Manage Decryption Exclusions (Continued)		
Step 2	Add a new decryption exclusion, or modify an existing one.	1. Select **Device > Certificate Management > SSL Decryption Exclusions**. 2. **Add** a new entry, or select an entry to modify it. 3. (**Custom exclusions only**) Enter the **hostname** of the website or application you want to exclude from decryption. This hostname is compared against the SNI requested by the client or the CN presented in the server certificate. To exclude all hostnames associated with a certain domain from decryption, you can use a wildcard asterisk (*). In this case, all sessions where the server presents a CN that contains the domain are excluded from decryption. Make sure that the hostname field is unique for each custom entry. If a predefined exclusion matches a custom entry, the custom entry takes precedence. 4. Optionally, select **Shared** to share the exclusion across all virtual systems in a multiple virtual system firewall. 5. **Exclude** the application from decryption, or clear this checkbox to start decrypting an entry that was previously excluded from decryption. 6. Click **OK** to save the new exclusion entry.
Step 3	Enable or disable one or more exclusions at a time.	1. Select **Device > Certificate Management > SSL Decryption Exclusions**. 2. Select one or more decryption exclusion entries. 3. Click **Enable** to exclude all selected entries from decryption, or **Disable** to turn on decryption for the selected entries.
Step 4	Remove outdated decryption exclusions.	Palo Alto Networks removes decryption exclusions from the list when they become obsolete (for example, when an application that decryption previously caused to break now supports decryption). However, if a predefined decryption exclusion is disabled, it is not automatically removed the list. Select **Show Obsoletes** to check if there are disabled, predefined exclusions on your list that Palo Alto Networks that are no longer needed.

Perfect Forward Secrecy (PFS) for Inbound SSL Sessions

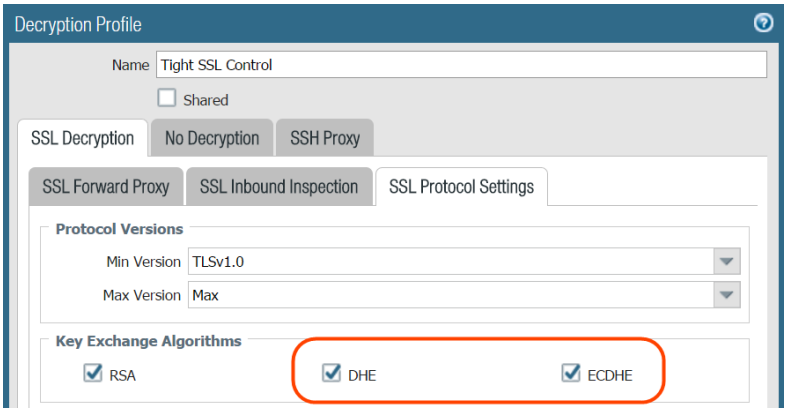
PFS support is now extended to sessions decrypted using SSL Inbound Inspection (PFS support for SSL Forward Proxy was introduced in PAN-OS 7.1). PFS is a secure communication protocol that prevents the compromise of one encrypted session from leading to the compromise of multiple encrypted sessions. With PFS, a server generates unique private keys for each secure session that it establishes with a client. If a server private key is compromised, only the single session established with that key is vulnerable—an attacker cannot retrieve data from past and future sessions because the server establishes each connection with a uniquely generated key.

This extended support for ephemeral Diffie-Hellman (DHE)-based PFS and elliptic curve Diffie-Hellman (ECDHE)-based PFS is enabled by default after the upgrade to PAN-OS 8.0—note that these settings were also enabled by default in PAN-OS 7.1, though in that release version, support covered only SSL Forward Proxy decrypted traffic.

If you use the DHE or ECDHE key exchange algorithms to enable PFS, you cannot use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.

Verify PFS Key Exchange Algorithms (DHE and ECDHE) Support

Step 1 Select **Objects > Decryption Profile**, **Add** or modify a profile, and select **SSL Decryption > SSL Protocol Settings** to view settings you can use to enable or disable **DHE** and **ECDHE** support for decrypted SSL sessions (ECDHE and DHE support are enabled by default).



Step 2 To confirm that the PFS settings are being applied to decrypted traffic, select **Decryption > Policies** and scan the Decryption Profile column. Check that the default decryption profile, or a custom profile like the profile in Step 1, is attached to a decryption policy rule.

	Source	Destination				
Name	Zone	Zone	URL Category	Action	Type	Decryption Profile
Sensitive Catego...	trust	untrust	financial-services health-and-medi... military shopping	no-decrypt	ssl-forward-proxy	Tight SSL control
Decrypt All Else	trust	untrust	any	decrypt	ssl-forward-proxy	default

Step 3 To learn more about setting up decryption for inbound SSL traffic, get started with SSL Inbound Inspection.

Virtualization Features

Seamless VM-Series Model Upgrade

You now have the ability to scale up and scale down the VM-Series capacity as bandwidth and capacity requirements change on your network by upgrading the model license. The upgrade process between different VM-Series models can be done with minimal downtime and intervention. Upgrading the VM-Series capacity does not require a reboot. Additionally, the serial number for the firewall does not change and no configuration is lost. For example, in an MSSP environment, if your tenant requires more capacity than the VM-100 supports, the MSSP can upgrade the firewall to a VM-300 without deactivating the license or changing the serial number of the firewall.

Upgrade the VM-Series Capacity	
Step 1	Enable automatic VM-Series license deactivation. You no longer have to manually deactivate a VM-Series license before upgrading he capacity. Before continuing with your upgrade, Install a License Deactivation API Key.
Step 2	Upgrade the license on the Customer Support portal. If you already have an authorization code for your VM-Series model, skip this step.
Step 3	Before you initiate the capacity upgrade, verify that you have allocated enough hardware resources to support the new VM-Series model. The process for assigning additional hardware resources differs for each hypervisor.
Step 4	Upgrade the capacity.
Step 5	Verify that your firewall capacity license upgrade is successful.

CloudWatch Integration for VM-Series Firewalls on AWS

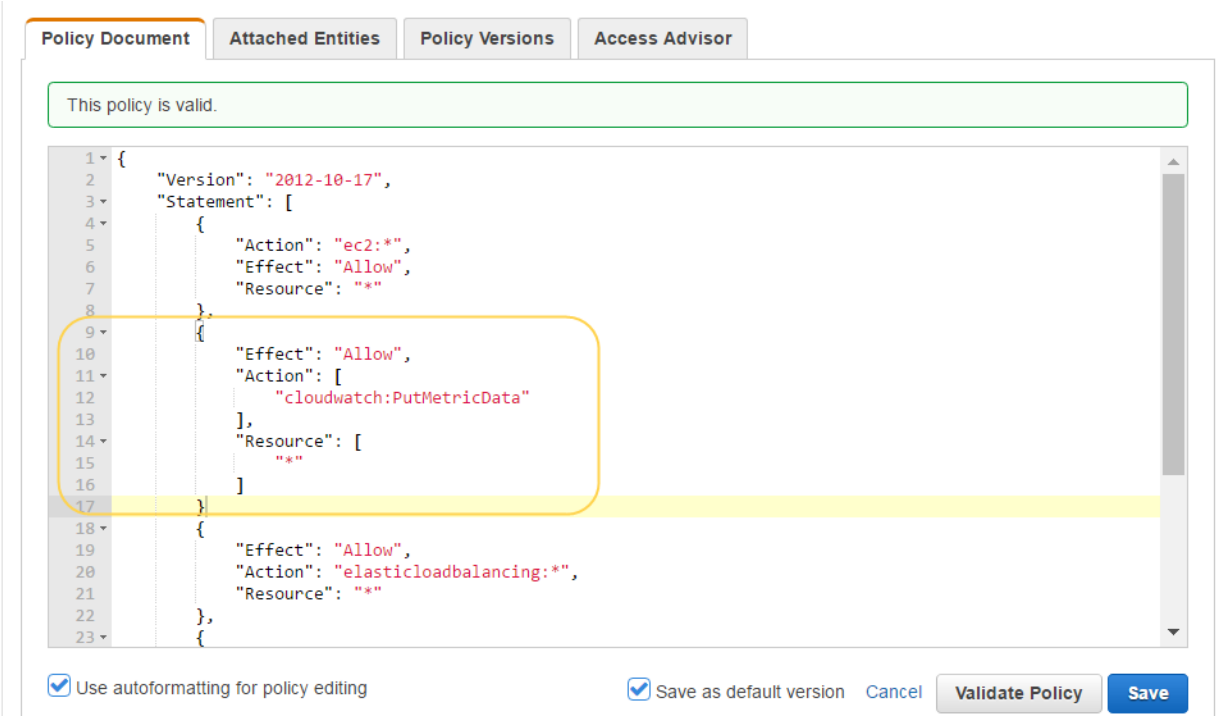
The VM-Series firewall on AWS can now publish native PAN-OS metrics to AWS CloudWatch at a specified time interval. You can use these metrics to make resource-driven decisions, such as take action to launch or terminate instances of the VM-Series firewalls based on usage.

Enable CloudWatch Monitoring on the VM-Series Firewall

Step 1 Assign the appropriate permissions for the AWS Identity and Access Management (IAM) user role that you use to deploy the VM-Series firewall on AWS.

Whether you launch a new instance of the VM-Series firewall or upgrade an existing VM-Series firewall on AWS to PAN-OS 8.0, the IAM role associated with your instance, must have permissions to publish metrics to CloudWatch.

1. On the AWS console, select **IAM > Policies** and click the **Policy Name** link associated with the IAM role you want to modify.
2. Edit the **Policy Document** to include the following permissions to the IAM role.



Enable CloudWatch Monitoring on the VM-Series Firewall (Continued)	
Step 2	Enable CloudWatch on the VM-Series firewall on AWS. 1. Log in to the web interface on the VM-Series firewall 2. Select **Device > Operations > AWS CloudWatch**. 3. Select **Enable CloudWatch Monitoring**. 4. Enter the **CloudWatch Namespace** to which the firewall can publish metrics. The namespace cannot begin with **`AWS`**. 5. Set the **Update Interval** to a value between 1-60 minutes. This is the frequency at which the firewall publishes the metrics to CloudWatch. The default is 5 minutes. 6. **Commit** the changes. Until the firewall starts to publish metrics to CloudWatch, you cannot configure alarms for PAN-OS metrics.
Step 3	Verify that you can see the metrics on CloudWatch. 1. On the AWS console, select **CloudWatch > Metrics**, to view CloudWatch metrics by category. 2. From the Custom Metrics drop-down, select the namespace. 3. Verify that you can see PAN-OS metrics in the viewing list.
Step 4	Configure alarms and actions for PAN-OS metrics on CloudWatch. For details, refer to the AWS CloudWatch documentation.

Support for NSX Security Tags on the VM-Series Firewall for NSX

The VM-Series for NSX now supports the tagging of guest VMs with NSX security tags due to the addition of the source and destination universally unique identifier (UUID) of guest VMs in your NSX deployment. Vmware vCenter passes the source and destination UUID to the VM-Series firewall via the Netx API and added to the threat and traffic logs. With this information in the logs, the firewall can be configured to tag infected guest VMs via the NSX Manager API.

Panorama receives predefined payload formats for NSX through content updates. These formats are available in the HTTP Server profile, which you can use to make an API call and trigger an automatic action on the NSX Manager. For example, whenever a threat log of critical severity is generated on the firewall, Panorama uses the API to communicate with the NSX Manager to tag the guest VM as infected. The NSX manager then dynamically moves the guest VM with the infected tag into a quarantined security group.

Configure Panorama to Dynamically Quarantine Infected Guests	
Step 1	Create a dynamic address to be your quarantine dynamic address group.
Step 2	Create an HTTP Server Profile to send API calls to NSX Manager. This server profile must send an HTTP PUT request to NSX Manager and use one of the predefined NSX payload formats.
Step 3	Define the match criteria for when Panorama will forward logs to the NSX Manager, and attach the HTTP server profile to use.
Step 4	Configure an NSX server certificate for Panorama to forward logs to NSX manager. Those server certificates must exported and uploaded to NSX Manager to allow for necessary communication to take place.
Step 5	Log in to vCenter and associate a security group with a security tag. The security tag your associate with your quarantine security group must match the payload format you configured in your HTTP Server profile.

VM-Series Firewall Performance Enhancements

PAN-OS 8.0 introduces three new VM-Series firewall models and increased performance, capacity, and efficiency of the existing VM-Series firewall models. The VM-Series firewalls now support a wider range of deployment scenarios and higher volumes of traffic when compared to previous versions of PAN-OS. These enhancements enable three broad use cases—optimized resources for customer-premises equipment (CPE) and network tenant environments, improved performance and efficiency for perimeter and east-west data center traffic, and maximized performance to support network function virtualization (NFV).

To support multitenancy for data centers and service providers, such as Managed Security Service Providers (MSSPs), the VM-Series firewall now supports oversubscription of CPUs as well as a smaller hardware footprint. This allows you to deploy multiple instances of the VM-Series firewall at a higher density on hypervisors running on x86 architecture.

VM-Series Model Capacity and Performance

- VM-100, VM-200, VM-300, and VM-1000-HV—The capabilities of the VM-200 and VM-1000-HV now match those of the VM-100 and VM-300, respectively. All existing models now support higher performance and much higher capacity than before on an optimized compute footprint.
- VM-500 and VM-700—These new models can utilize a larger compute resource footprint to achieve higher performance and capacity than other VM-Series firewall models.
- VM-50—A new virtual firewall model that delivers lower performance on a small hardware footprint and supports oversubscription of compute resources.

VM-Series Model	Sessions	Security Rules	Dynamic IP Addresses	Security Zones	IPSec VPN Tunnels	SSL VPN Tunnels
VM-50	50,000	250	1,000	15	250	250
VM-100 VM-200	250,000	1,500	2,500	40	1,000	500
VM-300 VM-1000-HV	800,000	10,000	100,000	40	2,000	2,000
VM-500	2,000,000	10,000	100,000	200	4,000	6,000
VM-700	10,000,000	20,000	100,000	200	8,000	12,000

Use the firewall comparison tool to view the maximum capacities and additional technical information about each VM-Series firewall model.

This release adds I/O enhancements through the support for Data Plane Development Kit (DPDK) for the VM-Series on KVM, ESXi, and AWS and Large receive offload (LRO) for the VM-Series firewall on NSX. Additionally, SR-IOV is now supported for ESXi.

DPDK enhances VM-Series performance by increasing NIC packet processing speed. On the VM-Series firewall, DPDK is enabled by default on KVM and ESXi. If you disable DPDK or it is disabled by default, packet mmap is used instead.

On AWS, DPDK is disabled by default. HA on AWS requires the adding and deleting of interfaces dynamically, which is not supported in DPDK. If you are not using HA, you can enable DPDK to increase performance.

All data interfaces must be using the same driver to support DPDK.

Hypervisor	Virtual Driver	Intel Driver
ESXi	VMXNET3	ixgbe, ixgbevf, i40e, i40evf
KVM	virtio	ixgbe, ixgbevf, i40e, i40evf
AWS	—	ixgbevf

LRO is a technique for increasing the inbound throughput on high-bandwidth network connections by decreasing CPU overhead. This release adds support for LRO on the VM-Series firewall on NSX. LRO is disabled by default on new NSX deployments and on upgrade to 8.0. You can enable or disable LRO and view the LRO status through the CLI.

VM-Series System Requirements

To support the increase in performance and scale, the minimum hardware resource requirements have changed.

VM-Series Model	Supported Hypervisors	Supported Cores	Minimum Memory	Minimum Hard Drive
VM-50	ESXi, KVM, Hyper-V	2	4.5GB	32GB
VM-100 VM-200	ESXi, KVM, Hyper-V, AWS, Azure, NSX	2	6.5GB	60GB
VM-300 VM-1000-HV	ESXi, KVM, Hyper-V, AWS, Azure, NSX	2, 4	9GB	60GB
VM-500	ESXi, KVM, Hyper-V, AWS, Azure, NSX	2, 4, 8	16GB	60GB
VM-700	ESXi, KVM, Hyper-V, AWS, Azure	2, 4, 8, 16	56GB	60GB

The way the VM-Series firewall utilizes allocated cores has changed in 8.0. The number of cores assigned to the management plane and those assigned to the dataplane differs depending on the total number of cores assigned to the VM-Series firewall. If you assign more cores than those officially supported for the model, any additional cores are assigned to the management plane.

Supported Cores	Management Plane Cores	Dataplane Cores
2	1	1
4	2	2
8	2	6
16	4	12

VM-Series Firewall CPU Oversubscription

This release introduces support for CPU oversubscription at ratios of 2:1, 3:1, 4:1, or 5:1 (maximum) on all VM-Series models. For example, a host machine with 16 physical CPU and at least 180GB of memory (40 × 4.5GB) can support up to 40 instances to the VM-50 at a 5:1 ratio. Each VM-50 requires two vCPUs and five VM-50s can be associated with each pair of CPUs. When planning your deployment, consider other functions, such as virtual switches, and guest machines on the host that require hardware resources of their own so they have the requisite hardware to operate.

Beyond meeting the minimum VM-Series System Requirements, no additional configuration is required to take advantage of oversubscription. Deploy the VM-Series as normal and resource oversubscription happens automatically.

DHCP on Management Interfaces and Hypervisor-Assigned MACs

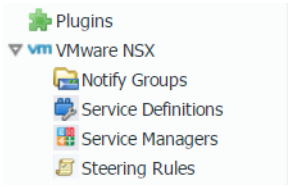
To aid in the deployment of large quantities of VM-Series firewalls, the VM-Series now has DHCP on management interfaces and hypervisor-assigned MAC addresses enabled by default on new installations with PAN-OS 8.0. With DHCP enabled on management interfaces, the VM-Series firewall is accessible immediately; there is no need to configure a management IP address on each firewall individually.

By enabling the use of a hypervisor-assigned MAC address, you do not need to enable promiscuous mode on the virtual switches in a layer3 deployment. VM-Series firewalls upgraded to 8.0 from a previous version do not have these enabled by default, you must perform a factory reset after upgrading or enable manually.

NSX VM-Series Configuration through Panorama

Beginning with 8.0, you can manage all security-related configuration for the VM-Series NSX integration through Panorama. The new workflow consolidates security configuration on Panorama, and decouples the need for continuous interaction between security and virtualization administrators. Panorama now provides NSX Manager with the contextual information required to secure traffic from guest virtual machines in SDDC environments. Dynamic address groups on Panorama map to security groups on NSX Manager, zones map to service profiles, and security policy rules map to steering rules.

These configuration changes take advantage of the new extensible plug-in architecture in Panorama. All the interface related to NSX integration are now part of the NSX plug-in and only display in Panorama when the plug-in is installed.

Configure the VM-Series Firewall for NSX With the VMware NSX Plugin	
Step 1	Install a VM-Series License Deactivation API Key on Panorama before configuring the VM-Series Edition on NSX. Deleting the Palo Alto Networks Service Deployment on NSX Manager automatically triggers license deactivation. A license API key is required to successfully deactivate the VM-Series license.
Step 2	Install the VMware NSX Plugin to access the configuration options for managing the VM-Series firewall on NSX. 

VM-Series Bootstrapping with Block Storage

You can now bootstrap the VM-Series firewall on ESXi, KVM, and Hyper-V using block storage. Support for block storage gives you an alternative to using an ISO or CD-ROM for deploying and attaching a bootstrap package to new instances of the VM-Series firewall.

Similar to bootstrapping the VM-Series in Azure, bootstrapping these other hypervisors using block storage requires that you create a Linux virtual machine to format and prepare the bootstrap package. See the VM-Series Deployment Guide for information about creating a bootstrap package.

Bootstrap the VM-Series Firewall with a Block Device	
Step 1	Create the bootstrap package and the block device. How you create the block device is different for each hypervisor: • ESXi • KVM • Hyper-V
Step 2	Deploy the firewall.
Step 3	Attach the bootstrap package to the firewall.
Step 4	Verify bootstrap completion.

VM-Series License Deactivation API Key

You are now required to install a license deactivation API key and enable the firewall to verify the identity of PAN update servers to deactivate a VM-Series firewall license. These changes provide additional security to the connection between your firewall or Panorama and the Palo Alto Networks Update and License server. You can retrieve your license API key from the Customer Support Portal and configure it using the CLI on the firewall and Panorama.

The Verify Update Server Identity option under Device > Setup > Services is enabled by default. Before deactivating an VM-Series firewall, verify that this option is enabled.

Install the License Deactivation API Key	
Step 1	Retrieve the license deactivation API key from the Customer Support Portal.
Step 2	Use the CLI to install the API key. `request license api-key set key <key>` Seamless VM-Series Model Upgrade and NSX VM-Series Configuration through Panorama both require the use of a license deactivation API key.
Step 3	Use the CLI to delete an installed API key if you need to replace it. `request license api-key delete` To deactivate a VM-Series firewall after deleting the API key, you must install a new one.
Step 4	Check that the firewall can **Verify Update Server Identity** at **Device > Setup > Services**.
Step 5	After installing the license API key, deactivate the VM-Series firewall as normal.

Networking Features

- Tunnel Content Inspection
- Multiprotocol BGP
- Zone Protection for Multi-path TCP (MPTCP) Evasions
- Zone Protection for Non-IP Protocols on a Layer 2 VLAN or Virtual Wire
- Zone Protection for SYN Data Payloads
- Static Route Removal Based on Path Monitoring
- IPv6 Router Advertisement for DNS Configuration
- NDP Monitoring for Fast Device Location
- Hardware IP Address Blocking
- Packet Buffer Protection
- Reconnaissance Protection Whitelist
- IKE Peer and IPSec Tunnel Capacity Increases

Tunnel Content Inspection

The firewall can now perform tunnel content inspection on the traffic content of cleartext tunnel protocols:

- Generic Routing Encapsulation (GRE) (RFC 2784)
- Non-encrypted IPSec traffic [NULL Encryption Algorithm for IPSec (RFC 2410) and transport mode AH IPSec]
- General Packet Radio Service (GPRS) Tunneling Protocol for User Data (GTP-U)

You can use tunnel content inspection to enforce Security, DoS Protection, and QoS policies on traffic in these types of tunnels and traffic nested within another cleartext tunnel. You can view inspected tunnel information to verify that tunneled traffic complies with your corporate security and usage policies.

- In enterprise environments, you can inspect traffic tunneled using GRE or non-encrypted IPSec. For security, QoS, and reporting reasons, you want to inspect the traffic inside the tunnel.
- In Service Provider environments, you can use GTP-U to tunnel data traffic from mobile devices. You want to inspect the inner content without terminating the tunnel protocol, and you want to record user data from users.

All firewall models support tunnel content inspection of GRE and non-encrypted IPSec. Only PA-5200 Series and VM-Series firewalls support tunnel content inspection of GTP-U.

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

Configure Tunnel Content Inspection		
Step 1	Create a Security policy to allow packets through the tunnel that use a specific application, such as GRE.	Configure a Security Policy Rule.
Step 2	Create a Tunnel Inspection policy that specifies the criteria for packets that meet the policy, the tunnel protocols to inspect, the maximum level of encapsulation to inspect, and separate security policies for tunnel zones, if you choose.	Configure Tunnel Content Inspection
Step 3	Use the ACC to view inspected tunnel activity.	View Inspected Tunnel Activity
Step 4	View Tunnel Inspection logs and other logs for tunnel inspection information.	View Tunnel Information in Logs
Step 5	Create a custom report about Tunnel Inspected traffic.	Create a Custom Report Based on Tagged Tunnel Traffic

Multiprotocol BGP

BGP supports IPv4 unicast prefixes, but a BGP network that uses IPv4 multicast routes or IPv6 unicast prefixes needs Multiprotocol BGP (MP-BGP) in order to exchange routes of address types other than IPv4 unicast. The firewall now supports MP-BGP, which means you have IPv6 connectivity to your BGP networks that use native IPv6 or dual stack IPv4 and IPv6. Service providers can offer IPv6 service to their customers, and enterprises can use IPv6 service from service providers.

MP-BGP uses Network Layer Reachability Information (NLRI) in a Multiprotocol Reachable NLRI attribute that the firewall sends and receives in BGP Update packets. The attribute contains information about the destination prefix:

- The Address Family Identifier (AFI) indicates that the destination prefix is an IPv4 or IPv6 address.
- The Subsequent Address Family Identifier (SAFI) in PAN-OS indicates that the destination prefix is a unicast or multicast address (if the AFI is IPv4), or that the destination prefix is a unicast address (if the AFI is IPv6). PAN-OS does not support IPv6 multicast.

If you enable MP-BGP for IPv4 multicast or if you configure an IPv4 multicast static route, the firewall supports separate unicast and multicast route tables for static routes. You might want to separate unicast and multicast traffic going to the same destination because, for example, your multicast traffic is critical, so you need it to take fewer hops or undergo less latency.

You can also exercise more control over how BGP functions by configuring BGP to use routes from only the unicast or multicast route table (or both) when BGP imports or exports routes, sends conditional advertisements, or performs route redistribution or route aggregation. You can also now Redistribute IPv6 Routes from BGP and OSPFv3.

Configure a BGP Peer with MP-BGP	
• Enable MP-BGP for a peer to use IPv4 or IPv6 unicast.	Configure a BGP Peer with MP-BGP for IPv4 or IPv6 Unicast
• Enable MP-BGP for a peer to use IPv4 multicast.	Configure a BGP Peer with MP-BGP for IPv4 Multicast
• Create a static route and install it in the unicast or multicast route table only.	Configure a Static Route
• View the unicast or multicast route table or the forwarding table. View the BGP RIB Out table (which shows the routes that the firewall sends to BGP neighbors).	Configure a BGP Peer with MP-BGP for IPv4 or IPv6 Unicast

Zone Protection for Multi-path TCP (MPTCP) Evasions

You can now enable or disable Multi-path TCP (MPTCP) globally or for each network zone. MPTCP is an extension of TCP that allows a client to simultaneously use multiple paths (instead of a single path) to connect with a destination host. MPTCP especially benefits mobile users, enabling them to maintain dual connections to both Wi-Fi and cellular networks as they move—this improves both the resilience and quality of the mobile connection and enhances the user experience. However, MPTCP can also potentially be leveraged by attackers as part of an evasion technique. This feature provides the flexibility to enable or disable MPTCP for all firewall traffic or for individual network zones, based on the visibility, performance, and security requirements for each network zone.

By default, MPTCP support is disabled on the firewall, and the firewall converts MPTCP connections to regular TCP connections. However, you can choose to enable MPTCP support globally or for certain network zones.

Enable or Disable MPTCP Support	
• For all firewall traffic.	You can use the following CLI command to enable or disable MPTCP support for firewall traffic: `set deviceconfig setting tcp strip-mptcp-option no / yes` • Enter **no** to enable MPTCP support (the firewall does not remove the MPTCP option field from packets). • (**Default**) Enter **yes** to convert MPTCP connections to TCP connections (the firewall removes the MPTCP option field from packets).
• For a network zone.	Zone protection profiles allow you to set up security between network zones. Following the upgrade to PAN-OS 8.0, both existing and new zone protection profiles are set to support MPTCP by default. Take the following steps to enable or disable MPTCP support for a specific network zone: 1. Select **Network > Network Profiles > Zone Protection** and modify or **Add** a zone protection profile. 2. Select **Packet Based Attack Protection > TCP Drop**. 3. Select one of the Multipath TCP (MPTCP) Options to apply to the network zone: • **no**—Enable MPTCP support (do not strip the MPTCP option). • **yes**—Disable MPTCP support (strip the MPTCP option). With this option configured, MPTCP connections are converted to standard TCP connections, as MPTCP is backwards compatible with TCP. • **global**—Support MPTCP based on the global MPTCP setting For all firewall traffic. 4. Click **OK** to save the profile. If MPTCP support is disabled globally, but you want to support MPTCP for certain network zones, make sure that you enable MPTCP for each zone through which traffic traverses.

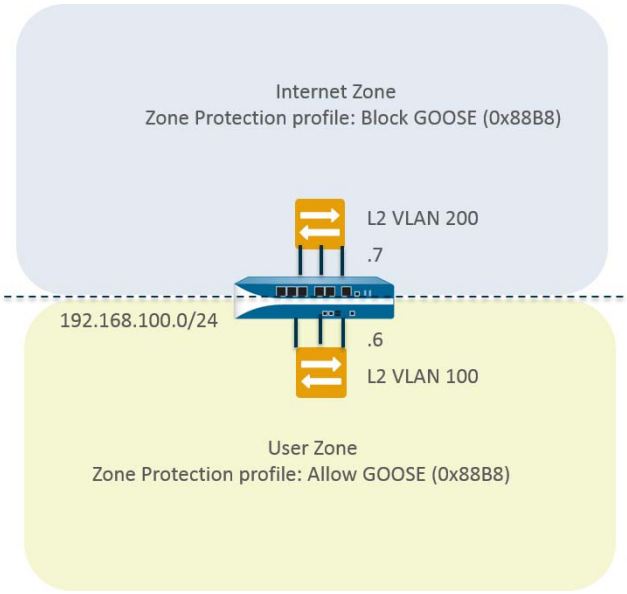
Zone Protection for Non-IP Protocols on a Layer 2 VLAN or Virtual Wire

You can now use a Zone Protection profile to block or allow non-IP protocols between security zones on a Layer 2 VLAN or a virtual wire. You can also block or allow such protocols between interfaces within a single zone on a Layer 2 VLAN. Controlling non-IP protocols for a zone reduces security risks and facilitates regulatory compliance by preventing these less secure protocol packets from entering a zone or interface in a zone where they don't belong.

Examples of non-IP protocols that you can control are AppleTalk, Banyan VINES, LLDP, NetBEUI, Spanning Tree, and Supervisory Control and Data Acquisition (SCADA) systems such as Generic Object Oriented Substation Event (GOOSE), among many others.

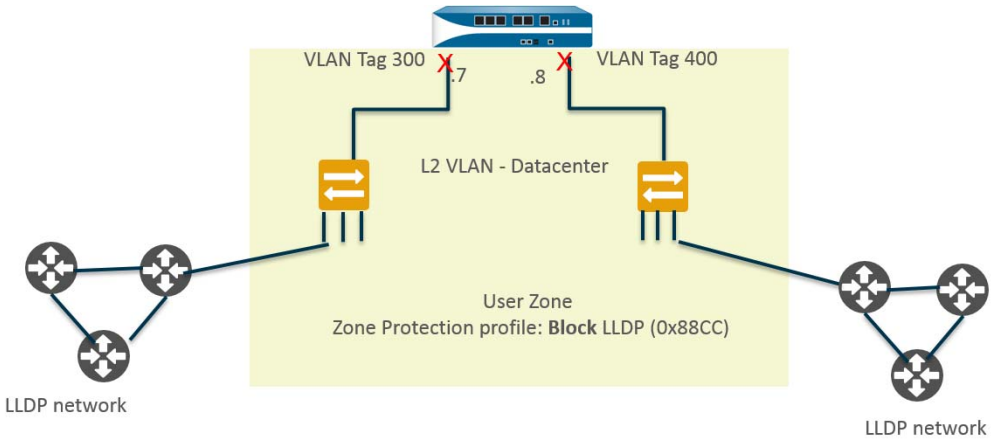
Enhance your zone protection by configuring protocol protection, which lists non-IP protocols for the firewall to either block (exclude) or allow (include). Apply the Zone Protection profile to an ingress security zone for physical interfaces or AE interfaces.

For example, a firewall in a Layer 2 VLAN can be divided into two subinterfaces, each belonging to a VLAN and a zone. You can whitelist the GOOSE protocol for one zone and blacklist it for the other zone, as shown in the following figure:



If you don't implement a Zone Protection profile with non-IP protocol control, the firewall allows non-IP protocols in a single zone to go from one Layer 2 interface to another. In the following intrazone example, blacklisting LLDP packets ensures that LLDP for one network does not discover a network reachable through another interface in the zone. The Layer 2 VLAN is divided into two subinterfaces and belongs to the User zone. By applying a Zone Protection profile that blocks LLDP to the User zone:

- Subinterface .7 blocks LLDP from its switch to the firewall at the red X on the left, preventing that traffic from reaching subinterface .8.
- Subinterface .8 blocks LLDP from its switch to the firewall at the red X on the right, preventing that traffic from reaching subinterface .7.



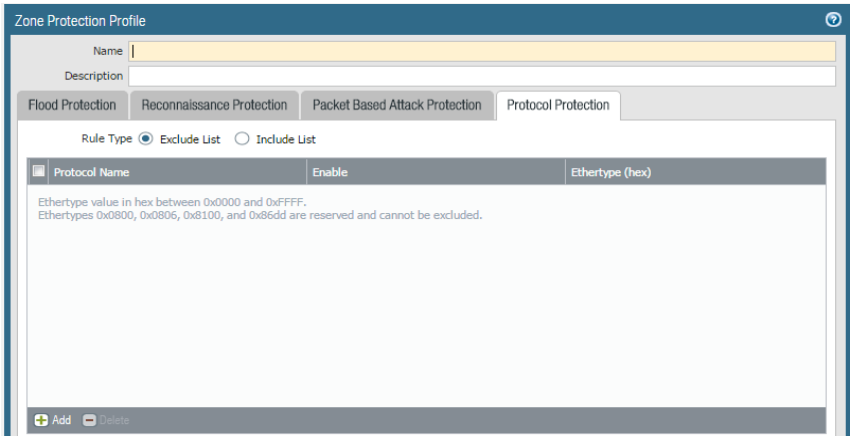
Each Include List or Exclude List you configure for protocol protection supports up to 64 Ethertype entries, identified by their IEEE hexadecimal Ethertype code. Locate the Ethertype codes you want to use at sources such as:

- http://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml
- http://standards-oui.ieee.org/ethertype/eth.txt
- http://www.cavebear.com/archive/cavebear/Ethernet/type.html

The firewall supports multiple Zone Protection profiles, one per zone. Protocol protection doesn't let you block IPv4 (Ethertype 0x0800), IPv6 (0x86DD), ARP (0x0806), or VLAN-tagged frames (0x8100). These Ethertypes are always implicitly allowed in an Include List without listing them and implicitly allowed even if you configure an Exclude List.

Configure Non-IP Protocol Protection for a Zone

Step 1 Configure non-IP Protocol Protection in a Zone Protection profile and apply the profile to an ingress security zone.



Step 2 Access the CLI to view the number of non-IP packets the firewall has dropped based on protocol protection.

```
> show counter global name pkt_nonip_pkt_drop
> show counter global name pkt_nonip_pkt_drop delta yes
```


Zone Protection for SYN Data Payloads

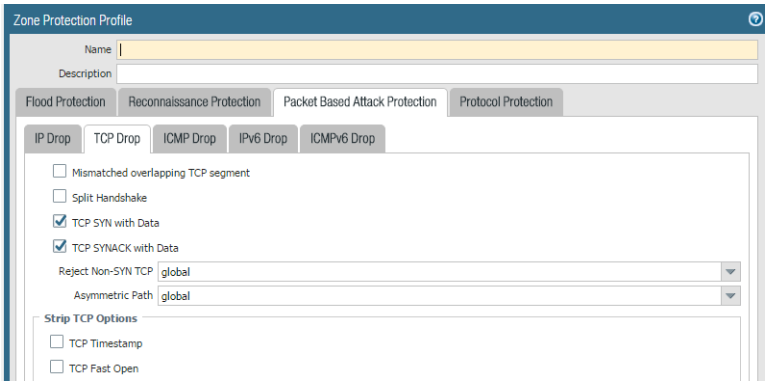
You can now use a Zone Protection profile for Packet Based Attack Protection to drop TCP SYN and SYN-ACK packets that contain data in the payload during a three-way handshake. A Zone Protection profile by default is set to drop SYN and SYN-ACK packets with data.

The TCP Fast Open option (RFC 7413) preserves the speed of a connection setup by including data in the payload of SYN and SYN-ACK packets. A Zone Protection profile treats handshakes that use the TCP Fast Open option separately from other SYN and SYN-ACK packets; the profile by default is set to allow the handshake packets if they contain a valid Fast Open cookie.

You can control how the Zone Protection profile handles these three options (SYN packets with data in the payload, SYN-ACK packets with data in the payload, and the TCP Fast Open option) independently of each other. As an alternative to the default Zone Protection behavior, you can create a Zone Protection profile to strip the TCP Fast Open option and data payload from SYN and SYN-ACK packets.

If you have existing Zone Protection profiles in place when you upgrade to PAN-OS 8.0, the three default settings will apply to each profile and the firewall will act accordingly.

Protect a Zone Against TCP SYN and SYN-ACK Packets with Data in Payload	
Step 1	Create a Zone Protection profile for Packet Based Attack Protection.
Step 2	Configure the profile to drop TCP SYN and SYN-ACK packets with data in the payload. 1. Select **TCP Drop**. 2. Select **TCP SYN with Data** to cause the firewall to drop SYN packets that contain data in the payload. Default is enabled. 3. Select **TCP SYNACK with Data** to cause the firewall to drop SYN-ACK packets that contain data in the payload. Default is enabled.



Protect a Zone Against TCP SYN and SYN-ACK Packets with Data in Payload (Continued)		
Step 3	Configure the profile to preserve TCP Fast Open support.	1. In the Strip TCP Option section, to allow a SYN or SYN-ACK with data and a cookie in the TCP Fast Open option (not strip the TCP Fast Open option or data), leave **TCP Fast Open** disabled (unchecked), which is the default.  In a Zone Protection profile with Flood Protection against SYN packets, you can configure the firewall to take action against a SYN flood by enabling **SYN Cookies**. In a zone protected by the **SYN Cookies** action, when the firewall receives a SYN from a client, rather than immediately sending the SYN to the server, the firewall generates a cookie (on behalf of the server) to send in the SYN-ACK to the client. The client responds with its ACK and the cookie; upon this validation the firewall then sends the SYN to the server. Because the firewall responds to the client on behalf of the server, it removes all data from the SYN (including TCP Fast Open) before responding to the client with its SYN-ACK. That is, **SYN Cookies** does not support TCP Fast Open when the firewall acts as a SYN proxy for the server. If you need TCP Fast Open support, don't use **SYN Cookies** as a SYN flood mitigation method; use **Random Early Drop** instead. 2. Click **OK**.
Step 4	Apply the Zone Protection profile to a security zone that is assigned to interfaces you want to protect.	1. Select **Network > Zones** and select the zone where you want to assign the Zone Protection profile. 2. **Add** the **Interfaces** belonging to the zone. 3. For **Zone Protection Profile**, select the profile you created. 4. Click **OK**.
Step 5	Commit.	Click **Commit**.

Step 6	Troubleshoot zone protection for a zone by viewing the TCP SYN, SYNACK and TCP Fast Open settings and the number of packets the firewall has dropped for each setting.	Access the CLI.
		`> show zone-protection zone <zone-name>`
		The following is sample output:
		`> show zone-protection zone user`
		`---------------------------------------------`
		`Number of zones with protection profile: 1`
		`---------------------------------------------`
		`Zone user, vsys vsys1, profile dos-protect-syn`
		`---------------------------------------------`
		`IPv(4/6)filter:`
		`discard-tcp-syn-with-data enabled: yes, packet dropped: 10`
		`discard-tcp-synack-with-data: enabled: yes, packet dropped: 20`
		`strip-tcp-fast-open-and data: enabled: yes, packet dropped: 30`

Static Route Removal Based on Path Monitoring

You can now use path monitoring so the firewall removes static route table entries when the link connection fails on the firewall interface to which the static route is assigned. Without path monitoring, if a path failure occurs upstream from the firewall, but the customer-premises equipment (CPE) keeps the link artificially active, the firewall can't detect the failure and doesn't update the static route in the route table; the firewall blackholes the traffic.

To inform the firewall when a static route is down, use static route removal based on path monitoring to detect when the path to one or more monitored destinations has gone down. The firewall can then reroute traffic using an alternative route.

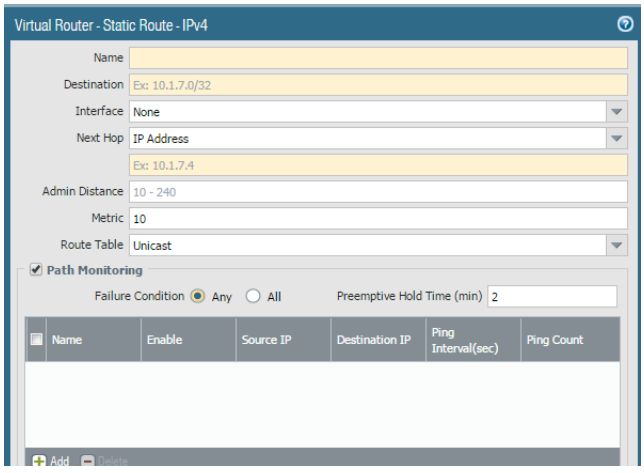
The firewall performs path monitoring by sending ICMP ping messages to one or more monitored destinations that you determine are reliable and reflect the availability of the static route. If pings to any (or all) of the monitored destinations fail, the firewall considers the static route down too and removes it from the RIB and FIB. The firewall selects an alternative static route to the same destination from the RIB and places it in the FIB. The firewall can reinstate a static route that has come back up, and then compare metrics of routes to the same destination to decide which route goes in the FIB.

Path monitoring is desirable to avoid blackholing traffic for:

- A static or default route.
- A static or default route redistributed into a routing protocol.
- A static or default route between two virtual routers in case one router has a problem (Bidirectional Forwarding Detection [BFD] doesn't function between virtual routers).
- A static or default route when one peer does not support BFD. (The best practice is not to enable both BFD and path monitoring for a single interface.)
- A static or default route instead of using PBF path monitoring, which doesn't remove a failed static route from the RIB, FIB, or redistribution policy.

Configure Path Monitoring for a Static Route

- Enable path monitoring and configure monitored destinations for a static route. View the RIB and FIB to verify that the static route is removed.
  Configure Path Monitoring for a Static Route



IPv6 Router Advertisement for DNS Configuration

Neighbor Discovery Protocol (NDP) functions for IPv6 in a capacity similar to ARP for IPv4. The firewall implementation of Neighbor Discovery (ND) allows you to provision IPv6 hosts with the Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) Options. You configure these DNS Options on the firewall so the firewall can provision your IPv6 hosts; therefore you don't need a separate DHCPv6 server to provision the hosts. The firewall sends IPv6 Router Advertisements (RAs) containing these options to IPv6 hosts as part of their DNS configuration to fully provision them to reach internet services. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration, describes the options.

- **Recursive DNS Server Addresses**—Recursive DNS refers to a series of DNS requests by an RDNS Server to resolve a domain name with an IP address. Configure the addresses of RDNS Servers so the firewall can advertise them and thus provision IPv6 hosts with the addresses of RDNS servers that can resolve their DNS queries. A single IPv6 RA uses one RDNS Server Option with multiple addresses and the same lifetime, or multiple RDNS Server Options with different lifetime values.
- **DNS Search List**—Configure a list of domain names (suffixes) that you want to advertise to a DNS client. The firewall thus provisions the DNS client to use the suffixes in its unqualified DNS queries. The DNS client appends the suffixes, one at a time, to an unqualified domain name before entering the name into a DNS query, thereby using a fully qualified domain name (FQDN) in the query. For example, if a user tries to submit a DNS query for the name "quality" without a suffix, the DNS client appends a period and the first DNS suffix from the DNS Search List to the name and transmits a DNS query. If the first DNS suffix on the list is "company.com", the resulting DNS query is for the FQDN "quality.company.com".

  If the DNS query fails, the client appends the second DNS suffix from the list to the unqualified name and transmits a new DNS query. The client uses the DNS suffixes in order until a DNS lookup succeeds (ignoring the remaining suffixes) or the client has tried all suffixes on the list. A single IPv6 RA uses one DNS Search List Option with multiple domain names and the same lifetime, or multiple DNS Search List Options with different lifetimes.

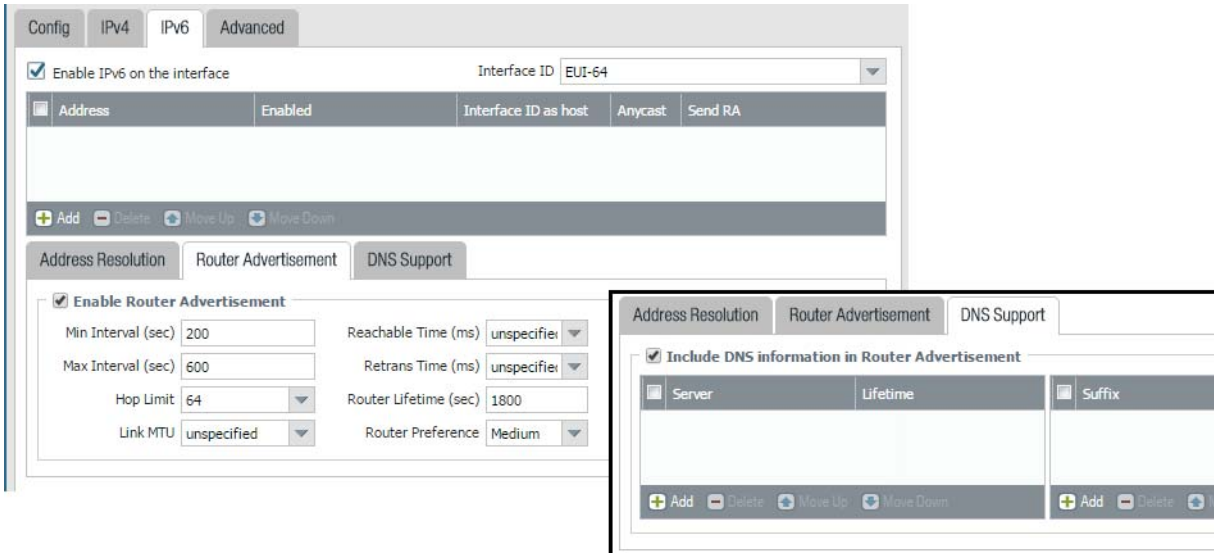
The capability of the firewall to send IPv6 RAs for DNS configuration allows the firewall to perform a role similar to DHCP, and is unrelated to the firewall being a DNS proxy, DNS client or DNS server.

Configure RDNS Servers and DNS Search List

- Configure Layer 3 Interfaces on the firewall to send IPv6 Router Advertisements, and specify the RDNS Server addresses and DNS suffixes for the firewall to advertise from this interface.

  IPv6 Router Advertisement for DNS Configuration is supported for Ethernet interfaces, subinterfaces, Aggregated Ethernet interfaces, and Layer 3 VLAN interfaces on all PAN-OS firewall models.

  Manage IPv6 Hosts Using NDP



NDP Monitoring for Fast Device Location

The firewall now provides NDP monitoring. You can quickly track a device and user who has violated a security policy rule by viewing, in one location, the IPv6 addresses of devices on the link local network, their MAC address, associated username from User-ID (if the firewall has a User-ID mapping), reachability Status of the address, and Last Reported date and time the NDP monitor received a Router Advertisement from this IPv6 address. The username is on a best-case basis; there can be many IPv6 devices on a network with no username, such as printers, fax machines, servers, etc. You need the MAC address that corresponds to the IPv6 address in order to trace the MAC address back to a physical switch or Access Point.

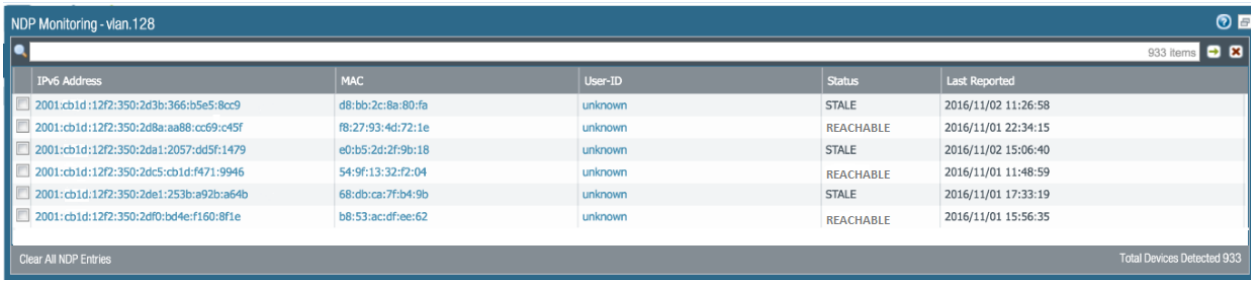
NDP monitoring is not guaranteed to discover all devices because there could be other networking devices between the firewall and the client that filter out NDP or Duplicate Address Detection (DAD) messages. The firewall can monitor only the devices that it learns about on the interface.

NDP monitoring also monitors Duplicate Address Detection (DAD) packets from clients and neighbors. You can also monitor IPv6 ND logs to make troubleshooting easier.

NDP monitoring is supported for Ethernet interfaces, subinterfaces, Aggregated Ethernet interfaces, and VLAN interfaces on all PAN-OS platforms.

Enable NDP Monitoring

- Enable NDP Monitoring and view information such as the IPv6 address of a neighbor the firewall has discovered, the corresponding MAC address, corresponding User ID (on a best-case basis), reachability Status of the address, and Last Reported date and time this NDP Monitor received an RA from this IP address.



Hardware IP Address Blocking

When the firewall blocks a source IP address, such as when you configure a **Classified** DoS Protection policy rule with the Action to **Protect**, or a Security policy with a Vulnerability Protection profile, the firewall automatically blocks that traffic in hardware before those packets use CPU or packet buffer resources.

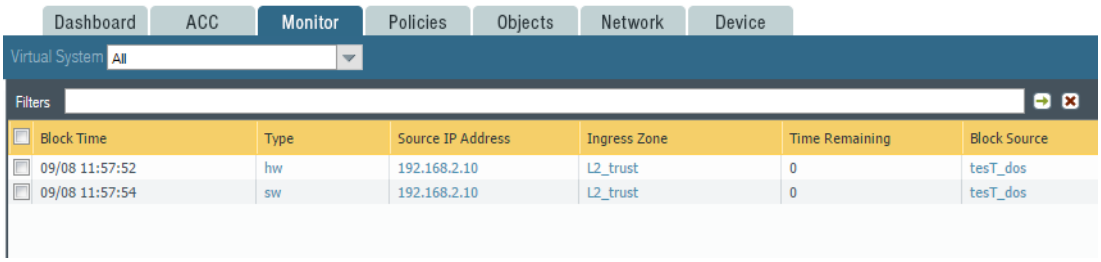
Hardware IP address blocking is supported on PA-3060 firewalls, PA-3050 firewalls, PA-5000 Series firewalls, PA-5200 Series firewalls, and PA-7000 Series firewalls.

You can Monitor Blocked IP Addresses, for example to get more information about an IP address on the block list, change how long hardware blocks IP addresses, and delete an IP address from the list if you think it shouldn't be blocked.

Monitor Blocked IP Addresses

Step 1 View block list entries.

1. Select **Monitor > Block IP List**.
   Entries on the block list indicate whether they were blocked by hardware (hw) or software (sw).
2. To view details about an address on the block list, hover over a Source IP address and click the down arrow link. Click the **Who Is** link, which displays Network Solutions Who Is information about the address.



Step 2 Delete block list entries.

You might want to delete an entry if you determine an IP address shouldn't be blocked. You should then revise the policy rule that caused the firewall to block the address.

1. Select **Monitor > Block IP List**.
2. Select one or more entries and click **Delete**.

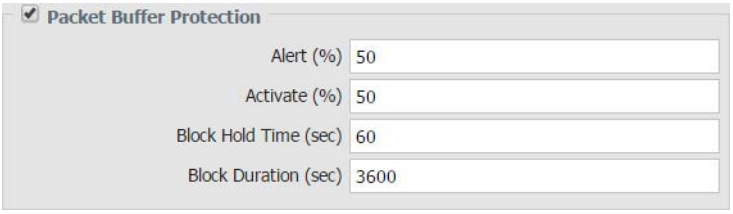
Packet Buffer Protection

To protect your firewall and network from single source denial of service (DoS) attacks that can overwhelm its packet buffer and cause legitimate traffic to drop, you can configure packet buffer protection. Packet buffer protection settings are configured globally and then applied per ingress zone. The firewall monitors how sessions utilize the packet buffer and then takes action against the session if it exceeds a configured percentage of utilization. As the various thresholds are met, the firewall takes increasingly severe action against the offending session or IP address.

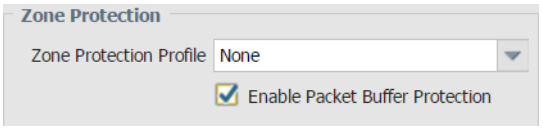
In addition to monitoring the buffer utilization of individual sessions, packet buffer protection can also block an IP address if certain criteria are met. While the firewall monitors the packet buffers, if it detects a source IP address rapidly creating sessions that would not individually be seen as an attack, action is taken against that address.

Configure Pack Buffer Protection

Step 1 Configure the global Packet Puffer Protection thresholds by selecting **Device > Setup > Sessions** and **Editing** the session settings.



Step 2 Enable Packet Puffer Protection on an ingress zone by selecting **Network > Zones** and clicking the name of a zone.



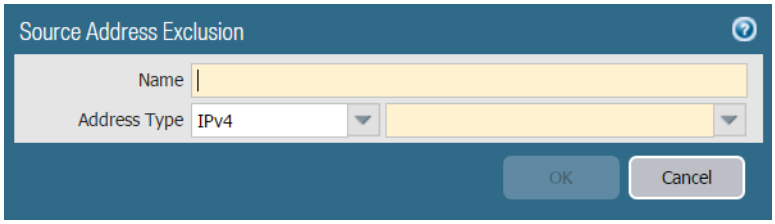
Reconnaissance Protection Whitelist

While ports scanning can be used for legitimate network monitoring purposes, it can also be used by attackers to search for an entry point into your network. To prevent such scanning attacks while still allowing you to use port scans, you can configure a source address exclusion whitelist. IPv4 or IPv6 IP addresses added to this whitelist are not blocked by the firewall when performing a port scan or host sweep. Any source address attempting to scan ports on your network are blocked.

Configure a Source Exclusion Whitelist

Step 1 Select **Network > Network Profiles > Zone Protection > Reconnaissance Protection** to add a source address exclusion whitelist to your zone protection Profile.

Step 2 Add an address to your source address exclusion whitelist. You add up to 20 IP addresses or netmask address objects.



IKE Peer and IPSec Tunnel Capacity Increases

The PA-7000 Series, PA-5000 Series, and PA-3000 Series firewalls now support more IKE peers and IPSec tunnels than in prior releases. The following table provides the capacities:

	PA-7000-20GXM-NPC PA-7000-20GQXM-NPC	PA-7000-20G-NPC PA-7000-20GQ-NPC	PA-5000 Series	PA-3000 Series
IKE Peers	4,000*	2,000*	2,000	2,000
IPSec Tunnels	12,000*	8,000*	8,000	3,000

*The capacities shown for PA-7000 Series firewalls are per chassis, regardless of how many Network Processing Cards (NPCs) are installed in the chassis. If a PA-7000 Series firewall uses only PA-7000-20GXM-NPC or PA-7000-20GQXM-NPC cards in the chassis, the higher capacities apply; otherwise, the lower capacities for the chassis apply.

Use the CLI operational command `show vpn ipsec-sa summary` to view summary information about IPSec tunnels.

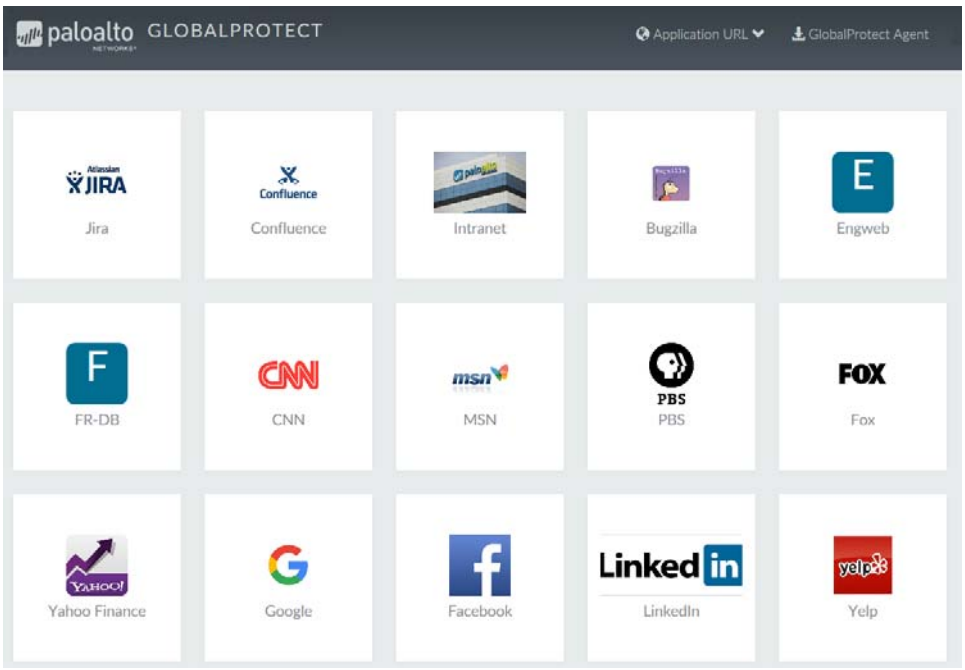
For better throughput and faster commit times, distribute the total number of IKE peers and IPSec tunnels among multiple interfaces.

GlobalProtect Features

Clientless SSL VPN

The public beta for GlobalProtect Clientless VPN is now available! Clientless VPN provides secure remote access to common enterprise web applications that use HTML, HTML5, and Javascript technologies. Users have the advantage of secure access from SSL-enabled web browsers without installing GlobalProtect client software. This is useful when you need to enable partner or contractor access to applications, and to safely enable unmanaged assets, including personal devices.

Figure: Sample Applications Landing Page for Clientless VPN

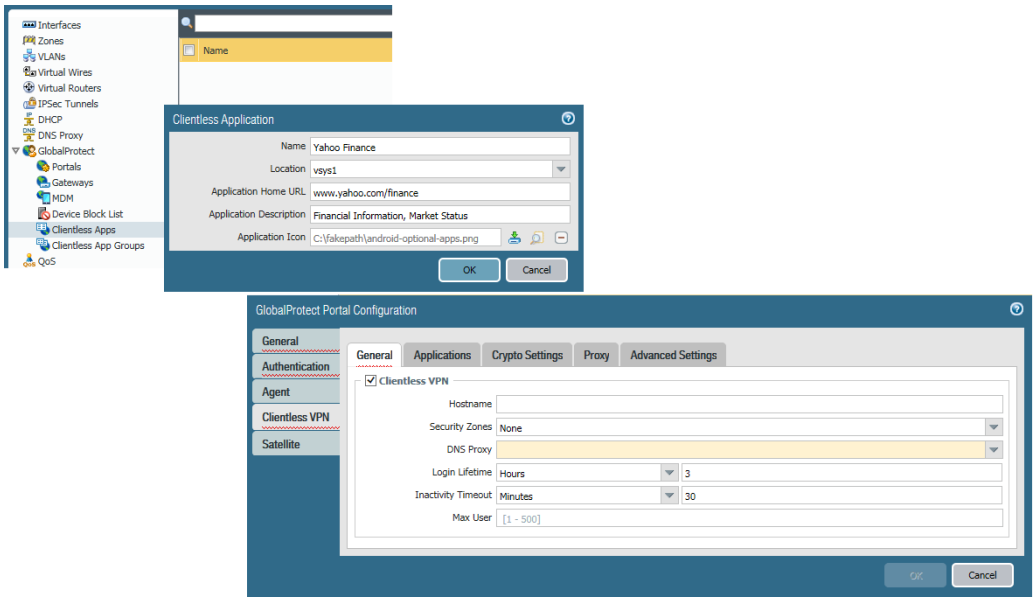


You can configure the GlobalProtect portal landing page to provide access to web applications based on users and user groups and also allow single-sign on to SAML-enabled applications. Supported operating systems are Windows, Mac, iOS, Android, Chrome, and Linux. Supported browsers are the latest versions of Chrome, Internet Explorer, Safari, and Firefox.

This feature also requires you to install a GlobalProtect subscription on the firewall that hosts the Clientless VPN from the GlobalProtect portal. You also need the **GlobalProtect Clientless VPN** dynamic updates to use this feature. Refer to Active Licenses and Subscriptions and Install Content and Software Updates.

When you configure Clientless VPN, remote users can log in to the GlobalProtect portal using a web browser and launch the web applications you publish for the user. Based on users or user groups, you can allow users to access a set of applications that you make available to them, or allow them to access additional corporate applications.

Figure: Configure Clientless VPN Applications

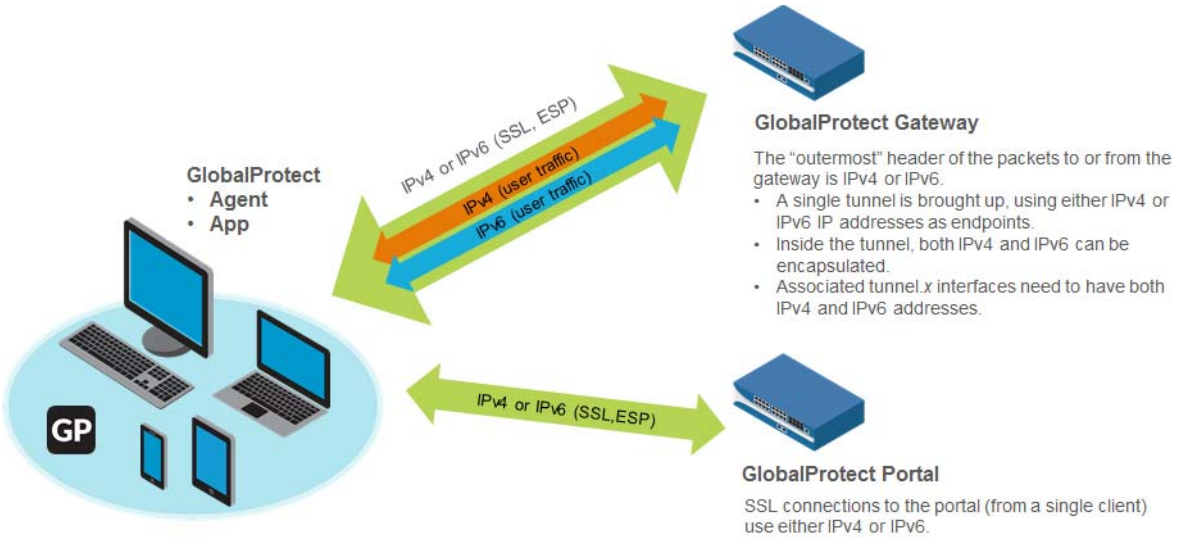


To configure Clientless VPN, follow these steps. Refer to the GlobalProtect 8.0 Administrator's Guide for more information on each step.

Configure Clientless VPN	
Step 1	Make sure you have a GlobalProtect subscription and the **GlobalProtect Clientless VPN** dynamic updates needed to use this feature.
Step 2	Configure the Clientless VPN applications and applications groups. The GlobalProtect portal displays these applications on the landing page that users see when they log in.
Step 3	Configure the GlobalProtect Portal to provide the Clientless VPN service.
Step 4	Map users and user groups to applications. This mapping controls which applications users or user groups can launch from a GlobalProtect Clientless VPN session. For information on qualified applications, see Supported Technologies.
Step 5	Specify the security settings for a Clientless VPN session. These settings control the authentication and encryption algorithms for the SSL sessions between the firewall and the published applications.
Step 6	If you need to reach the applications through a proxy server, specify one or more proxy server configurations to access the applications.
Step 7	Specify any special treatment for application domains. In some cases, the application may have pages that do not need to be accessed through the portal.
Step 8	Configure a Security policy rule to enable users to access the published applications.

IPv6 for GlobalProtect

GlobalProtect clients and satellites can now connect to portals and gateways using IPv6. This feature allows connection from clients that are in IPv6-only environments, IPv4-only environments, or dual-stack (IPv4 and IPv6) environments. The tunnel endpoints are IPv6 capable and IPv6 user traffic can be routed through the tunnel. You can encapsulate IPv4 traffic within an IPv6 tunnel and the IP address pool can assign both IPv4 and IPv6 addresses. This feature requires you to install a GlobalProtect subscription on any portal or gateway that uses IPv6.



IPv6 uses 16-byte hexadecimal number fields separated by colons (:) to represent the 128-bit addressing format. For example, `2001:db8:130D:0000:0000:09F0:876A:130B`.

To make an IPv6 address easier to represent, IPv6 uses the following conventions to shorten the address:

- Leading zeros in the address field are optional. For example, the following hexadecimal numbers can be represented as shown:
  - `0000` (expanded) can be represented as `0` (compressed)
  - `2001:db8:130D:0000:0000:09F0:876A:130B` (expanded) can be represented as `2001:db8:130D:0:0:9F0:876A:130B` (compressed)
- A pair of colons (`::`) represents successive fields of zeros. The pair of colons can be used only once in an IPv6 address. For example:
  - `E2001:db8:130D:0:0:9F0:876A:130B` (expanded) can be represented as `2001:db8:130D::9F0:876A:130B` (compressed)
  - `DD01:0:0:0:0:0:1` (expanded) can be represented as `DD01::1` (compressed)

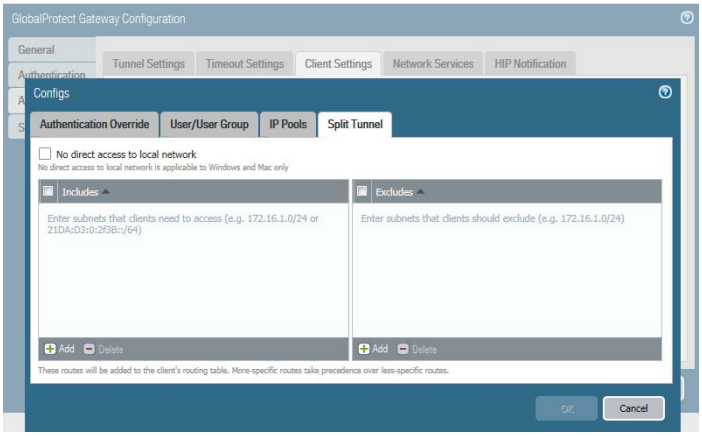
An address parser can easily identify the number of missing zeros in an IPv6 address by separating the two parts of the address and filling in the zeros until the 128-bit address is complete. However, if two colons (`::`) are placed in the same address, then there is no way to identify the size of each block of zeros. The use of colons makes many IPv6 addresses very small.

Configure an IP Address		
Step 1	Before you configure an IP address, select the type of GlobalProtect connection you want to configure.	Select the type of GlobalProtect connection you want to configure. This can include connections to the GlobalProtect portal, GlobalProtect internal gateways, GlobalProtect external gateways, authentication server IP pools, and tunnel interfaces to satellites.
Step 2	Navigate to **Network Settings** for the connection type. For portal and gateway configurations, **Network Settings** are located on the **General** tab. For satellite configurations, there is a **Network Settings** tab.	1. Choose the **IP Address Type** from the drop down. The IP address type can be **IPv4** (for IPv4 traffic only), **IPv6** (for IPv6 traffic only, or **IPv4 and IPv6.** Use **IPv4 and IPv6** if your network supports dual stack configurations, where IPv4 and IPv6 run at the same time. 2. Enter the **IP Address**. The IP address you enter must be compatible with the IP address type. For example, `172.16.1/0` for IPv4 addresses or `21DA:D3:0:2F3B` for IPv6 addresses. For dual stack configurations, enter both an IPv4 and IPv6 address.

Split Tunnel to Exclude by Access Route

You can now exclude specific destination IP subnet traffic from being sent over the VPN tunnel. With this feature, you can send latency sensitive or high bandwidth consuming traffic outside of the VPN tunnel while all other traffic is routed through the VPN for inspection and policy enforcement by the GlobalProtect gateway.

Now, the routes you send through the VPN tunnel can be defined either as the routes you include in the tunnel, or as routes that you exclude from the tunnel, or a combination of both. For example, you can set up split tunneling to allow remote users to access the internet without going through the VPN tunnel. More specific routes take precedence over less-specific routes. If you don't include or exclude routes, every request is routed through the tunnel (no split tunneling).

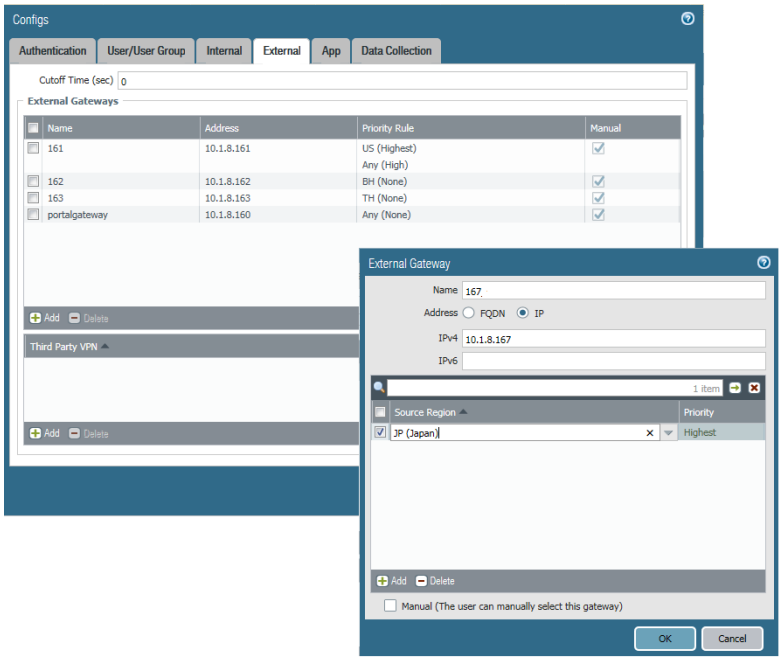


Configure a Split Tunnel by Excluding Access Routes	
Step 1	Configure the GlobalProtect gateway • Select the gateway you want to modify, or add a new gateway. • Enable tunneling and configure the tunnel parameters for an agent configuration.
Step 2	On the GlobalProtect Gateway Configuration dialog, select **Agent > Client Settings** to add or modify client settings for the agent.
Step 3	Select **Client Settings > Split Tunnel** to define a split tunnel configuration for the client. With a split tunnel, you can define the traffic that flows through the VPN by including routes, excluding routes, or both. In some cases, it can be easier to specify the routes you want the client to exclude, rather than specifying all the routes you want to include. For example, if you want to tunnel everything except one or two class C networks, you can exclude these few networks rather than compiling a long list of the networks you want to include. If you only exclude routes, all other routes are included by default. If you only include routes, all other routes are excluded by default. In the case of a conflict between included and excluded routes, the more specific route configuration will be honored.
Step 4	Make sure **No direct access to local network** is disabled. This setting disables split tunneling for networks on Windows and Mac OS.

Configure a Split Tunnel by Excluding Access Routes (Continued)	
Step 5	(**Optional**) In the **Includes** area, **Add** the destination subnets or address object (of type **IP Netmask**) to route only some traffic—likely traffic destined for your LAN—to GlobalProtect. These are the routes the gateway pushes to the remote users' endpoint and thereby determines what traffic the users' endpoint can send through the VPN connection.
Step 6	(**Optional**) In the **Excludes** area, **Add** the destination subnets or address object (of type **IP Netmask**) that you want the client to exclude. These routes will be sent through the endpoint's physical adapter rather than through the virtual adapter (the tunnel). Excluded routes should be more specific than the included routes; otherwise, you may exclude more traffic than you intended.  Excluding routes is not supported on Android. Only IPv4 routes are supported on Chrome.
Step 7	Save the gateway configuration. • Click **OK** twice • **Commit** your changes.

External Gateway Priority by Source Region

GlobalProtect can now use the geographic region of the GlobalProtect client to determine the best external gateway. By including source region as part of external gateway selection logic, you can ensure that users connect to gateways that are preferred for their current region. This can help avoid distant connections when there are momentary fluctuations of network latency. This can also be used to ensure all connections stay within a region if desired.

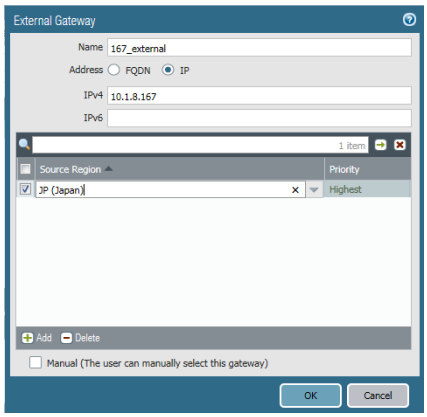


This feature is not supported for IPv6 connections. Also, identifying the region for the connecting endpoint may not be reliable if a proxy server is used for the portal connection or if the firewall performs a source NAT on the traffic to the portal.

Configure External Gateway Priority by Source Region	
Step 1	Define a GlobalProtect Agent Configuration.
Step 2	On the **External** tab, click **Add** for External Gateways.

Configure External Gateway Priority by Source Region (Continued)

Step 3 **Add** one or more **Source Regions** for the gateway, or select **Any** to make the gateway available to all regions. When users connect, GlobalProtect recognizes the device region and only allows uses to connect to gateways that are configured for that region. GlobalProtect prioritizes the source region first, and then considers gateway priority.



Step 4 Set the **Priority** of the gateway:

If you have only one external gateway, you can leave the value set to **Highest** (the default).

If you have multiple external gateways, you can modify the priority values (ranging from **Highest** to **Lowest**) to indicate a preference for the specific user group to which this configuration applies. For example, if you prefer that the user group connects to a local gateway you would set the priority higher than that of more geographically distant gateways. The priority value is then used to weight the agent's gateway selection algorithm.

If you do not want agents to automatically establish tunnel connections with the gateway, select **Manual only**. This setting is useful in testing environments.

Step 5 Save the agent configuration.

- Click **OK** twice
- **Commit** your changes.

Internal Gateway Selection by Source IP Address

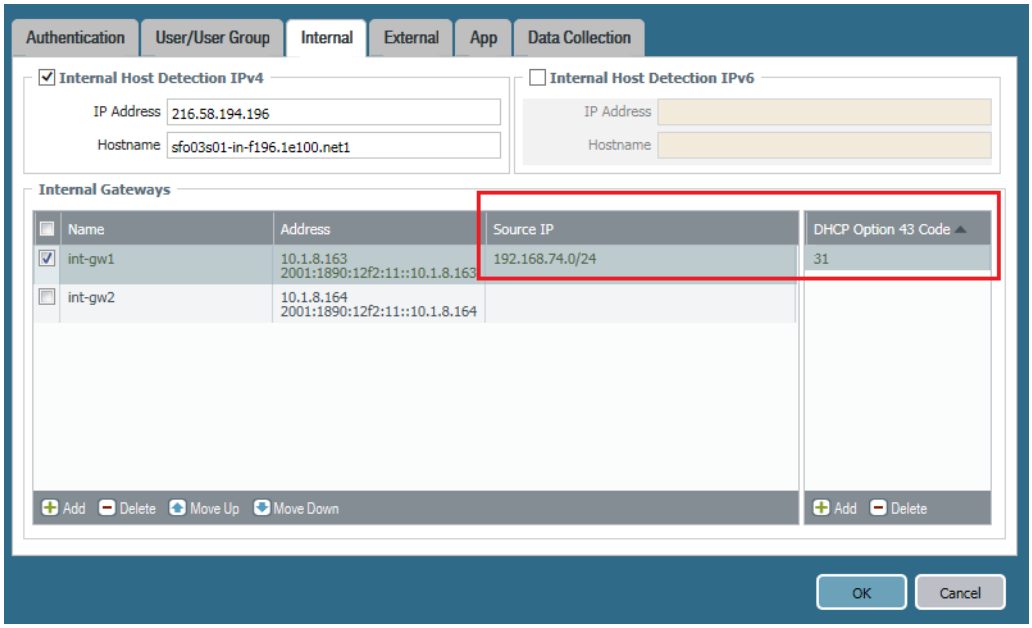
GlobalProtect can now restrict internal gateway connection choices based on the source IP address of the client. In a distributed enterprise, this feature allows users from a branch authenticate and send HIP reports to the firewall configured as the internal gateway for that branch as opposed to authenticating and sending HIP reports to all branches. Previously, to prevent GlobalProtect applications from sending HIP information to a large number of gateways, you had to configure multiple portals.

With this feature, internal gateway selection is based on the following considerations:

- The source IP address of the connecting endpoint. The GlobalProtect client only authenticates to internal gateways which are configured to accept connections from selected ranges of IP addresses.
- If the connecting endpoint uses DHCP for IP addressing, the GlobalProtect client authenticates to internal gateways based on a list of gateways obtained as an option from a DHCP server.

When both the source address and DHCP options are configured, the list of available gateways presented to the client is based on the combination (union) of the two configurations.

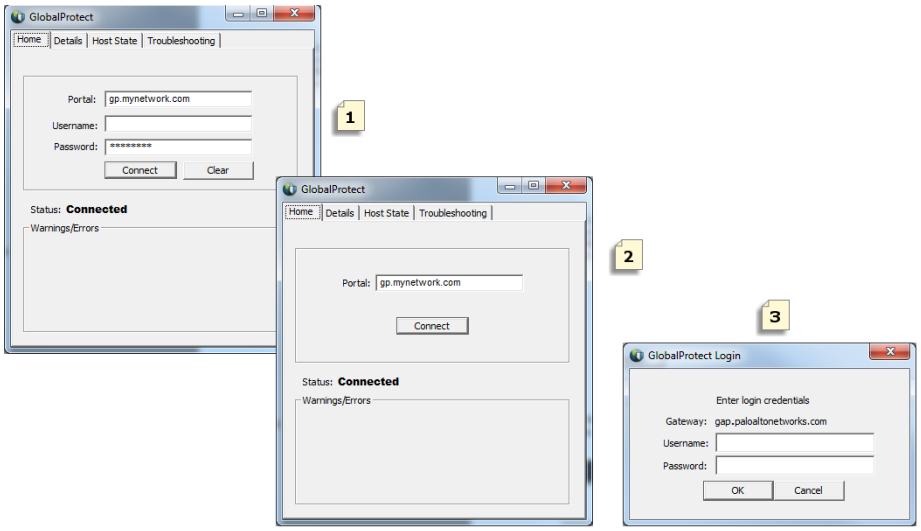
Configure Internal Gateway Priority by Source Region	
Step 1	Define a GlobalProtect Agent Configuration.
Step 2	On the **Internal** tab, **Add** a new internal gateway configuration for the agent, or modify an existing internal gateway configuration.
Step 3	(**Optional**) **Add** one or more **Source Addresses** to the gateway configuration. The source address can be an IP subnet or range. It can also be a predefined address. When users connect, GlobalProtect recognizes the source address of the device and only allows users to connect to gateways that are configured for that address.
Step 4	Click **OK** to save your changes.



Configure Internal Gateway Priority by Source Region (Continued)	
Step 5	(**Optional**) **Add** a **DHCP Option 43 Code** to the gateway configuration. You can include one or more sub-option codes associated with the vendor-specific information (Option 43) that the DHCP server has been configured to offer the client. For example, you might have a sub-option code 100 that is associated with an IP address of 192.168.3.1. When a user connects, the GlobalProtect portal sends the list of option codes in the portal configuration to the GlobalProtect agent and the agent selects gateways indicated by the options. When both the source address and DHCP options are configured, the list of available gateways presented to the client is based on the combination (union) of the two configurations.  DHCP options are supported on Windows and Mac endpoints only. DHCP options cannot be used to select gateways that use IPv6 addressing.
Step 6	Save the agent configuration. • Click **OK**. • **Commit** your changes.

GlobalProtect Agent Login Enhancement

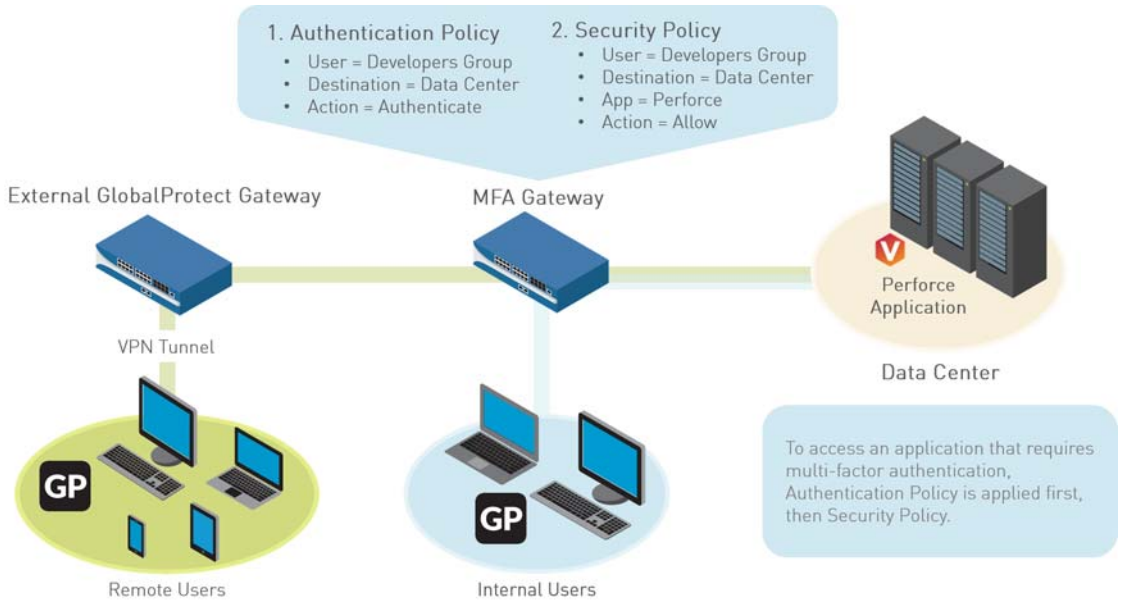
To simplify GlobalProtect agents and prevent unnecessary login prompts when a username and password are not required, the panel that showed portal, username, and password is now split into two screens (one screen for the portal location and another screen for username and password). The GlobalProtect agent now displays login prompts for username and password only if this information is required. GlobalProtect automatically hides the username and password screen for authentication types—such as cookie or client certificate authentication—that do not require a username and password.



Item	Description
1	The GlobalProtect agent login screen has been simplified. The username and password have been moved to a separate screen.
2	(**New**) This is the new, simplified screen for connecting to GlobalProtect and changing portals.
3	(**New**) The username and password prompts appear only if this information is required. These prompts are hidden automatically based on authentication type (for example, with cookie or certificate authentication).

Authentication Policy and Multi-Factor Authentication for GlobalProtect

You can now leverage the new Authentication Features within GlobalProtect to support access to non-browser-based applications that require multi-factor authentication. On Windows and Mac endpoints, GlobalProtect can now notify and prompt the user to perform the timely, multi-factor authentication needed to access sensitive network resources.



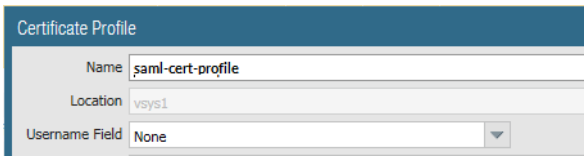
A GlobalProtect client is a requirement for multi-factor authentication on non-browser applications. For browser-based applications that require multi-factor authentication, users are automatically presented with Authentication Portal page (previously called the Captive Portal page). For non-browser applications, if a session matches an Authentication policy rule, then the firewall will send a UDP notification to the GlobalProtect client with an embedded URL link to the Authentication Portal page. GlobalProtect displays this message as a pop up notification to the user.

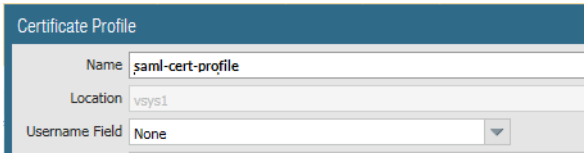
You can customize the message that GlobalProtect users see when prompted to authenticate. Clicking this link sends the user to the Authentication Portal page where they can start the multi-factor authentication process (the same as with browser-based HTTP applications).

Configure GlobalProtect to Display MFA Notifications	
Step 1	Before you configure GlobalProtect, configure multi-factor authentication on the firewall. To use multi-factor authentication for protecting sensitive resources, the easiest solution is to integrate the firewall with an MFA vendor that is already established in your network. When your MFA structure is ready, you can start configuring the components of your authentication policy. For more information, refer to Configure Multi-Factor Authentication. • Enable Captive Portal to record authentication timestamps and update user mappings. • Create server profiles that define how the firewall will connect to the services that authenticate users. • If you are using two-factor authentication with GlobalProtect to authenticate to the gateway or portal, a RADIUS server profile is required. If you are using GlobalProtect to notify the user about an authentication policy match (UDP message), a Multi Factor Authentication server profile is sufficient. • Assign the server profiles to an Authentication profile which specifies authentication parameters. • Configure a Security policy rule that allows users to access the resources that require authentication.
Step 2	For GlobalProtect to support multi-factor authentication on external gateways, you must configure a response page on the tunnel interface. Refer to Authentication Policy and Multi-Factor Authentication for more information on how to configure an MFA Login response page.
Step 3	Configure GlobalProtect clients to display multi-factor authentication notifications for non-browser-based applications on Windows and Mac endpoints. In an App configuration, configure the following settings: • **Enable Inbound Authentication Prompts from MFA Gateways** to **Yes**. To support multi-factor authentication (MFA), a GlobalProtect client must receive and acknowledge UDP prompts that are inbound from the gateway. Select **Yes** to enable a GlobalProtect client to receive and acknowledge the prompt. By default, the value is set to **No** meaning GlobalProtect will block UDP prompts from the gateway. • Specify the **Network Port for Inbound Authentication Prompts (UDP)** a GlobalProtect client uses to receive inbound authentication prompts from MFA gateways. The default port is 4501. To change the port, specify a number from 1 to 65535. • Specify the list of **Trusted MFA Gateways** a GlobalProtect client will trust for multi-factor authentication. When a GlobalProtect client receives a UDP message on the specified network port, GlobalProtect displays an authentication message only if the UDP prompt comes from a trusted gateway. • Configure the **Default Message for Inbound Authentication Prompts**. GlobalProtect automatically appends the URL of the Authentication Portal page you configured in the first step to the message.
Step 4	Save the agent configuration (click **OK** twice), and then **Commit** your changes.

SAML 2.0 Authentication for GlobalProtect

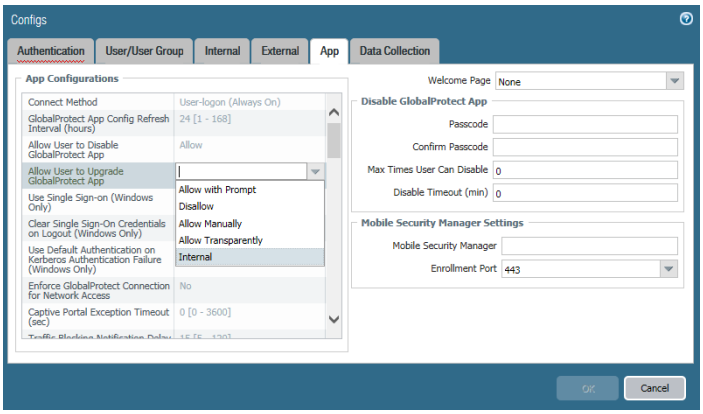
GlobalProtect portals, gateways, and clients now support SAML 2.0 Authentication. If you have chosen SAML as your authentication standard, GlobalProtect portals and gateways can act as a Security Assertion Markup Language (SAML) 2.0 service provider and GlobalProtect clients can authenticate users directly to the SAML identity provider. You can configure SAML authentication for user authentication to GlobalProtect gateways or to the GlobalProtect portal, or both.

Configure GlobalProtect Gateways and Portal for SAML User Authentication		
Step 1	Configure SAML 2.0 Authentication on the PAN-OS firewall that hosts the portal or gateway.	• Create a server profile with settings for access to the SAML 2.0 authentication service. • Create an authentication profile that refers to the SAML server profile.
Step 2	**(Optional)** Configure a GlobalProtect gateway.	1. Specify SAML authentication for gateway users: • Select **Authentication Profile** and add the SAML authentication profile you created in Step 1. This profile is used to authenticate an endpoint seeking access to the gateway. For iOS clients, SAML authentication is only supported when the **Connect Method** is configured for **On-demand (Manual user initiated connection)**. • Enter an **Authentication Message** to help end users understand which credentials to use when logging in. The message can be up to 100 characters in length (default is `Enter login credentials`). 2. (Optional) Select a **Certificate Profile** to use for client authentication to the gateway. For the certificate profile you select, make sure the **Username Field** in the certificate profile is set to **None**. 

Configure GlobalProtect Gateways and Portal for SAML User Authentication	
Step 3 (**Optional**) Define the GlobalProtect Client Authentication Configurations on the GlobalProtect portal.	3. Specify SAML authentication for the client: • Select **Authentication Profile** and add a SAML authentication profile. You can use the same profile you created in Step 1 or create a new SAML profile for the portal. This profile is used to authenticate an endpoint seeking access to the portal. • Enter an **Authentication Message** to help end users understand which credentials to use when logging in. The message can be up to 100 characters in length (default is `Enter login credentials`). 4. (**Optional**) Select a **Certificate Profile** to use for client authentication to the portal. For the certificate profile you select, make sure the **Username Field** in the certificate profile is set to **None**. 

Restrict Transparent Agent Upgrades to Internal Network Connections

As part of a GlobalProtect portal configuration, you can now control when transparent upgrades occur for a GlobalProtect client. With this configuration, if the user connects from outside the corporate network, the upgrade is postponed. Later, when the user connects from within the corporate network, the upgrade is activated. This feature allows you to hold the updates until users can take advantage of good network availability and high bandwidth from within the corporate network. The upgrades will not hinder users when they travel to environments with low bandwidth.

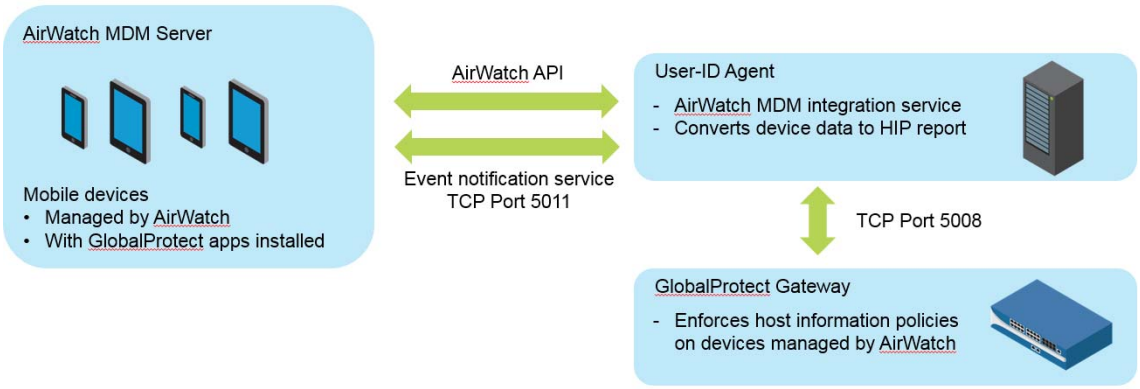


Restrict Transparent Agent Upgrades to Internal Network Connections	
• Customize the GlobalProtect Agent. The **App** configurations display the options with default values that you can customize for each client configuration. By default, GlobalProtect prompts the end user to upgrade.	To change the default behavior so that upgrades occur automatically, without interaction with the user, set **Allow User to Upgrade GlobalProtect App** to one of the following: • **Allow Transparently**—Upgrades occur automatically without interaction with the user. Upgrades can occur when the user is working remotely or connected from within the corporate network. • **Internal**—Upgrades occur automatically without interaction with the user, provided the user is connected from within the corporate network. This setting is recommended to prevent slow upgrades in low-bandwidth situations. When a user connects outside the corporate network, the upgrade is postponed and re-activated later when the user connects from within the corporate network. You must configure internal gateways and internal host detection to use this option. Upgrades for **Allow Transparently** and **Internal** occur only if the GlobalProtect software version on the portal is more recent than the GlobalProtect software version on the endpoint. For example, a GlobalProtect 3.1.3 agent connecting to a GlobalProtect 3.1.1 portal is not upgraded.

AirWatch MDM Integration

The Windows-based User-ID agent has been extended to support a new AirWatch MDM integration service. This service enables GlobalProtect to use the host information collected by the service to enforce HIP-based policies on devices managed by AirWatch. Running as part of the Windows-based User-ID agent, the AirWatch MDM integration service uses the AirWatch API to collect information from mobile devices that are managed by VMware AirWatch and translate this data into host information.

For Android devices managed by AirWatch, this feature supports Android for Work devices, but it does not support other types of Android devices.



MDM integration service included with the Windows-based User-ID agent does a full HIP query to the AirWatch MDM server to get the complete host information for a device. When a mobile device running the GlobalProtect app is connected to a GlobalProtect gateway, GlobalProtect can apply security policies with host information profiles.

You configure the MDM integration service to fetch AirWatch device information at regular intervals and push this information to GlobalProtect gateways. In addition, the service can monitor AirWatch event notifications and fetch updated device information when AirWatch events occur (for example, device enrollment, device wipe, and compliance changes). Refer to the *GlobalProtect Administrator's Guide* for information on how to configure AirWatch MDM integration.

PAN-OS XML API Features

- Admin-Level Commit and Revert using API
- SAML 2.0 Authentication using API
- CloudWatch Integration for VM-Series Firewalls on AWS using API
- Listing of Deactivation License Token Using API

Admin-Level Commit and Revert using API

The PAN-OS XML API now supports Admin-Level Commit and Revert for firewall or Panorama configuration changes. Use the API within your script, application, or service to automate firewall and Panorama configuration changes without affecting pending changes by other administrators.

Commit or Revert Admin-Level Changes using API
• **Commit admin-level changes on a firewall or Panorama while excluding shared objects**—Include the administrator name in the request. `https://firewall/api/?key=apikey&type=commit&action=partial&cmd=<commit><partial><device-and-network>excluded</device-and-network><shared-object>excluded</shared-object><admin><member>admin-name</member></admin></partial>`
• **Revert admin-level changes on a firewall**—Include the administrator name in the request. `https://firewall/api/?key=apikey&type=op&cmd=<revert><config><partial><admin><member>admin-name</member></admin></partial></config></revert>`
• **Revert admin-level changes to Panorama by a specific administrator within a specific device group**—Include the administrator name and the device group where Panorama will revert changes. `https://panorama/api/?key=apikey&type=op&cmd=<revert><config><partial><admin><member>admin-name</member></admin><device-group><member>device-group-name</member></device-group><no-template/><no-template-stack/><no-log-collector-group/><no-log-collector/><device-and-network>excluded</device-and-network></partial></config></revert>`

SAML 2.0 Authentication using API

You can now automate the configuration of SAML 2.0 Authentication single sign-on (SSO) and single logout (SLO) using the PAN-OS XML API. Programmatically create necessary SAML 2.0 authentication profiles using the API in your application, script, or enterprise portal.

Configure SAML SSO and SLO using API

- **(Recommended) Import a metadata file from the IdP**— The metadata file contains registration information and the certificate that the IdP uses to sign SAML messages. If you import a metadata file, you do not need to independently Create a SAML Identity Provider (IdP) server profile. Include the metadata filepath and SAML server profile name in your GET request:
  - **key**: API key
  - **file**: filepath to SAML metadata file. The metadata file contains registration information, as well as the certificate that the IdP uses to sign SAML messages. Export the metadata file from the IdP to a client system that the firewall can access. The certificate specified in the file must meet the certain SAML 2.0 Authentication requirements. Refer to your IdP documentation for instructions.
  - **profile-name**: passphrase, up to 31 characters

```
curl -F file=@filename.txt -g
'https://firewall/api/?key=apikey&type=import&category=idp-metadata&profile-name=profi
lename'
```

- **Create a SAML Identity Provider (IdP) server profile**

  Include IdP configuration parameters in your GET request:
  - **key**: API key
  - **vsys**: location, example values: shared, vsys1, vsys2
  - **name**: server profile name
  - **entity-id**: identity provider id
  - **certificate**: **(Best Practice)** identity provider certificate
  - **sso-url**: identity provider SSO URL
  - **slo-url:** identity provider SLO URL
  - **sso-binding:** SSO SAML HTTP binding, acceptable values: post, redirect
  - **ssl-binding:** SSL SAML HTTP binding, acceptable values: post, redirect
  - **max-clock-skew**: difference in system time as measured in seconds between firewall and IdP. The default value is 60 with a range of 1-900.
  - **validate-idp-certificate**: **(Best Practice)** specify whether you want to validate the IdP certificate. The default value is yes.
  - **want-auth-requests-signed**: specify whether the IdP expects a digital signature on authentication requests. The default value is no.

```
https://firewall/api/?key=apikey&type=config&action=set&xpath=/config/shared/server-pr
ofile/saml-idp/entry[@name='server-profile-name']&element=<certificate>cert-name</cert
ificate><entity-id>https://example.com/sso</entity-id><sso-url>https://example.com/sso
</sso-url><sso-bindings>post</sso-bindings><slo-url>https://example.com/slo</slo-url><
slo-bindings>post</slo-bindings><max-clock-skew>max-clock-skew</max-clock-skew><valida
te-idp-certificate>yes</validate-idp-certificate><want-auth-requests-signed>yes</want-
auth-requests-signed>
```

Configure SAML SSO and SLO using API (Continued)

- **Create a SAML authentication profile using the PAN-OS XML API**—Include SAML authentication profile parameters in your GET request:
  - **key**: API key
  - **authentication-profile:** authentication profile name
  - **enable-single-logout:** specify whether you want to enable SAML single logout. The default value is no.
  - **request-signing-certificate:** request signing certificate name
  - **server-profile:** SAML Identity Provider (IdP) server profile name
  - **certificate-profile:** certificate profile name
  - **attribute-name-username:** SAML username attribute
  - **attribute-name-usergroup:** SAML user group attribute
  - **attribute-name-access-domain:** SAML admin domain attribute
  - **attribute-name-admin-role:** SAML admin role attribute

```
https://firewall/api/?key=apikey&type=config&action=set&xpath=/config/shared/authentication-profile/entry[@name='authentication-profile-name']/method/saml-idp&element=<enable-single-logout>no</enable-single-logout><request-signing-certificate>certificate-name</request-signing-certificate><server-profile>server-profile-name</server-profile><certificate-profile>profile-name</certificate-profile><attribute-name-username>username</attribute-name-username><attribute-name-usergroup>usergroup</attribute-name-usergroup><attribute-name-access-domain>access-domain</attribute-name-access-domain><attribute-name-admin-role>admin-role</attribute-name-admin-role>
```

- **Add users and user groups that are allowed to authenticate with this authentication profile**—Include profile name and member list in your request:
  - **key**: API key
  - **authentication-profile:** authentication profile name
  - **member**: users or user groups. To include specific users or group, include them in brackets: `[member1, member3]`. To include all users, include `all`.

```
https://firewall/api/?key=apikey&type=config&action=set&xpath=/config/shared/authentication-profile/entry[@name='authentication-profile-name']/allow-list&element=<member>all</member>
```

- **Assign the authentication profile to firewall services that require authentication**—For example, to assign the authentication profile to a superuser administrator account for web access, include these parameters in your GET request:
  - **key**: API key
  - **name**: admin username
  - **authentication-profile**: name of the SAML authentication profile

```
https://firewall/api/?key=apikey&type=config&action=set&xpath=/config/mgt-config/users/entry[@name='adminname']&element=<permissions><role-based><superuser>yes</superuser></role-based></permissions><authentication-profile>authprofilename</authentication-profile>
```


CloudWatch Integration for VM-Series Firewalls on AWS using API

The PAN-OS XML API now supports CloudWatch Integration for VM-Series Firewalls on AWS.

Enable or Disable CloudWatch Integration for VM-Series Firewalls on AWS using API
• **Enable CloudWatch Integration for VM-Series Firewalls in AWS using API**—Include the AWS CloudWatch namespace and optionally the update interval in minutes (the default is 5) in your request: `https://firewall/api/?key=apikey&type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/aws-cloudwatch/&element=<enabled>yes</enabled><name>aws-cloudwatch-namespace</name><timeout>update-interval</timeout>`
• **Disable CloudWatch Integration for VM-Series Firewalls in AWS using API**—Include the AWS CloudWatch namespace in your request and set the <enabled> parameter to no: `https://firewall/api/?key=apikey&type=config&action=set&xpath=/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/aws-cloudwatch/&element=<enabled>no</enabled><name>aws-cloudwatch-namespace</name>`

Listing of Deactivation License Token Using API

When you manually deactivate a VM or a feature license or subscription on the firewall, you can now use the PAN-OS XML API to list and view token files.

- **List License Tokens on the Firewall**

  Parameters: firewall, key

  To view a a list of license token files on a firewall using the PAN-OS XML API, issue an operational request and include the firewall IP address or domain name along with the API key. Learn how to get started with the PAN-OS XML API.

  Request:

  https://*firewall*/api/?key=*apikey*&?type=op&cmd=<show><license-token-files/></show>

  Sample API request for listing license tokens using Curl:

```
curl -k -g
"https://1.2.3.4/api/?key=136484645546454684 6?type=op&cmd=<show><license-token-files
/></show>"
```

  Sample API response:

```
<response status="success">
<result>
<files>
<entry name="dact_lic.12022016.060130.tok"/>
<entry name="dact_lic.12282016.070001.tok"/>
</files>
</result>
</response>
```

- **View the Contents of a License Token on the Firewall**

  Parameters: firewall, key, name

  To view an individual token file on a firewall using the PAN-OS XML API, issue an operational request and include the firewall IP address or domain name, API key, and the name of the specific token file.

  Request:

  https://*firewall*/api/?key=*apikey*&?type=op&cmd=<show><license-token-files><name>*token_file.tok*</name></license-token-files></show>

  Sample API request for showing a license token using Curl:

```
curl -k -g
"https://1.2.3.4/api/?key=136484645546454684 6?type=op&cmd=<show><license-token-files
><name>dact_lic.12022016.060130.tok</name></license-token-files></show></operations>
</request>
```

  Sample API response:

```
<response status="success">
<result>lFDkWuqqjoNLJPjTaq1r6Tvoe_AtvOMSBpxgUzZPQJ7ZC7I7hz/QLlKLQIuGBa7U~pM027_yfjwj
vlIogX1qrXVag/nCUmsuYWTf5zqLn5Rgiulfgz9GNkN6eiRKFbYYQ~KlB2MENu1kKCxgZCUk7Gt/tYjC...
<!--TRUNCATED-->
</result>
</response>
```

