# PAN-OS ® New Features Guide

## *Version 9.1*

paloaltonetworks.com/documentation

techDOCS paloalto NETWORKS®

## Contact Information

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

## About the Documentation

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

## Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

## Last Revised

October 2, 2020

# Table of Contents

# Upgrade to PAN-OS 9.1

# Upgrade/Downgrade Considerations

The following table lists the new features that have upgrade or downgrade impact. Make sure you understand all upgrade/downgrade considerations before you upgrade to or downgrade from a PAN-OS 9.1 release. For additional information about PAN-OS 9.1 releases, refer to the PAN-OS 9.1 Release Notes.

**Table 1: PAN-OS 9.1 Upgrade/Downgrade Considerations**

| Feature | Upgrade Considerations | Downgrade Considerations |
|---|---|---|
| **SD-WAN Plugin**<br>The SD-WAN plugin provides intelligent, dynamic path selection on top of the industry leading security provided by PAN-OS | Enabling your SD-WAN plugin and starting your device creates SD-WAN databases. | Downgrading from PAN-OS 9.1 to an earlier version deletes any SD-WAN databases and removes any SD-WAN specific configurations. Your subscription remains on the device and is re-enabled if you upgrade. |
| **Upgrading a PA-7000 Series Firewall with a first generation switch management card (PA-7050-SMC or PA-7080-SMC)** | Before upgrading the firewall, run the following CLI command to check the flash drive's status: **`debug system disk-smart-info disk-1`**.<br>If the value for attribute ID #232, **Available_Reservd_Space 0x0000**, is greater than 20, then proceed with the upgrade. If the value is less than 20, then contact support for assistance. | Before downgrading the firewall, run the following CLI command to check the flash drive's status: **`debug system disk-smart-info disk-1`**.<br>If the value for attribute ID #232, **Available_Reservd_Space 0x0000**, is greater than 20, then proceed with the downgrade. If the value is less than 20, then contact support for assistance. |
| **Username in HTTP Header Insertion Entries** | None. | Downgrading from PAN-OS 9.1 removes the dynamic fields header values containing the domain and username. |
| **Dynamic User Groups** | None. | Downgrading from PAN-OS 9.1 migrates existing dynamic user groups to XML API user groups, retaining all group members at the time of the downgrade. The firewall continues to enforce any policy rules that apply to these groups. |
| **Option to Hold Web Requests During URL Category Lookup** | If you have this feature enabled, upgrading to PAN-OS 9.1 from an earlier version disables this option. Configure URL Filtering to re-enable this feature. | If you have this feature enabled, downgrading from PAN-OS 9.1 to an earlier version disables this option. |
| **URL Filtering BrightCloud Support** | With PAN-OS 9.1, BrightCloud is no longer supported as a URL Filtering vendor. Before you can | |

| Feature | Upgrade Considerations | Downgrade Considerations |
|---|---|---|
| | upgrade to PAN-OS 9.1, you'll first need to contact your sales representative to convert your BrightCloud URL Filtering license to a PAN-DB URL Filtering license. Only upgrade to PAN-OS 9.1 after confirming that the PAN-DB URL Filtering license is active on your firewall. | |
| **Enhanced Logging for GlobalProtect** | When upgrading to PAN-OS 9.1, any existing GlobalProtect logs stay in their current location, however any new logs received after the upgrade are stored in their new locations and categorized by the new GlobalProtect log type. | Any GlobalProtect logs collected after the upgrade will be lost when downgrading from PAN-OS 9.1 to an earlier version. |
| **Identity Provider Certificate**<br>(PAN-OS 9.1.3 or later) | Ensure that you configure the signing certificate for your SAML Identity Provider as the **Identity Provider Certificate** before you upgrade to PAN-OS 9.1.3 or later so that your users can continue to authenticate successfully. Always configure the Identity Provider Certificate when you configure your SAML authentication and, as a best practice, enable certificate validation when available. | |
| **Log Storage Quota** | On upgrade to PAN-OS 9.1, the firewall log storage quota (**Device** > **Setup** > **Management** > **Logging and Reporting Settings**) exceeds 100% of the total disk space available and causes commits to fail.<br>After you successfully upgrade a firewall to PAN-OS 9.1, modify the log storage quota to equal 100%.<br>1. Launch the firewall web interface.<br>2. Select **Device** > **Setup** > **Management** > **Logging and Reporting** and modify the log storage quota.<br>3. Access the firewall CLI. | |

| Feature | Upgrade Considerations | Downgrade Considerations |
|---|---|---|
|  | 4. Commit the configuration changes.<br>`admin# commit force` |  |

# Upgrade the Firewall to PAN-OS 9.1

How you upgrade to PAN-OS 9.1 depends on whether you have standalone firewalls or firewalls in a high availability (HA) configuration and, for either scenario, whether you use Panorama to manage your firewalls. Review the PAN-OS 9.1 Release Notes and then follow the procedure specific to your deployment:

- Determine the Upgrade Path to PAN-OS 9.1
- Upgrade Firewalls Using Panorama
- Upgrade a Standalone Firewall to PAN-OS 9.1
- Upgrade an HA Firewall Pair to PAN-OS 9.1

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

*Additionally, it is not recommended to manage firewalls running a later maintenance release than Panorama as this may result in features not working as expected. For example, it is not recommended to manage firewalls running PAN-OS 9.1.1 or later maintenance releases if Panorama is running PAN-OS 9.1.0.*

## Determine the Upgrade Path to PAN-OS 9.1

When you upgrade from one PAN-OS feature release version to a later feature release, you cannot skip the installation of any feature release versions in the path to your target release. In addition, the recommended upgrade path includes installing the latest maintenance release in each release version before you install the base image for the next feature release version. To minimize downtime for your users, perform upgrades during non-business hours.

*For manual upgrades, you must install the base image for a feature release before you upload and install a maintenance release image.*

Determine the upgrade path as follows:

STEP 1 | Identify which version is currently installed.

- From Panorama, select **Panorama** > **Managed Devices** and check the Software Version on the firewalls you plan to upgrade.
- From the firewall, select **Device** > **Software** and check which version has a check mark in the Currently Installed column.

STEP 2 | Identify the upgrade path:

*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.*

| Installed PAN-OS Version | Recommended Upgrade Path to PAN-OS 9.1 |
|---|---|
| 9.0.x | If you are already running a PAN-OS 9.0 release, download and install the preferred PAN-OS 9.0 maintenance release and reboot. You can then proceed to Upgrade the Firewall to PAN-OS 9.1. |

| Installed PAN-OS Version | Recommended Upgrade Path to PAN-OS 9.1 |
|---|---|
| 8.1.x | □ Download and install the latest preferred PAN-OS 8.1 maintenance release and reboot.<br>□ Download PAN-OS 9.0.0<br>□ Download and install the latest preferred PAN-OS 9.0 maintenance release and reboot.<br>□ Proceed to Upgrade the Firewall to PAN-OS 9.1. |
| 8.0.x | □ Download and install PAN-OS 8.0.20 and reboot.<br>□ Download PAN-OS 8.1.0.<br>□ Download and install the latest preferred PAN-OS 8.1 maintenance release and reboot.<br>□ Download PAN-OS 9.0.0<br>□ Download and install the latest preferred PAN-OS 9.0 maintenance release and reboot.<br>□ Proceed to Upgrade the Firewall to PAN-OS 9.1. |
| 7.1.x | □ Download and install the PAN-OS 7.1.26 maintenance release and reboot.<br>□ Download PAN-OS 8.0.0.<br>□ Download and install PAN-OS 8.0.20 and reboot.<br>□ Download PAN-OS 8.1.0.<br>□ Download and install the latest preferred PAN-OS 8.1 maintenance release and reboot.<br>□ Download PAN-OS 9.0.0<br>□ Download and install the latest preferred PAN-OS 9.0 maintenance release and reboot.<br>□ Proceed to Upgrade the Firewall to PAN-OS 9.1. |

## Upgrade Firewalls Using Panorama

Review the PAN-OS 9.1 Release Notes and then use the following procedure to upgrade firewalls that you manage with Panorama. This procedure applies to standalone firewalls and firewalls deployed in a high availability (HA) configuration.

*If Panorama is unable to connect directly to the update 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.*

Before you can upgrade firewalls from Panorama, you must:

□ Make sure Panorama is running the same or a later PAN-OS version than you are upgrading to. You must upgrade Panorama and its Log Collectors to 9.1 before upgrading the managed firewalls to this version. In addition, when upgrading Log Collectors to 9.1, you must upgrade all Log Collectors at the same time due to changes in the logging infrastructure.

□ Plan for an extended maintenance window of up to six hours when upgrading Panorama to 9.1. This release includes significant infrastructure changes, which means that the Panorama upgrade will take longer than in previous releases.

□ Ensure that firewalls are connected to a reliable power source. A loss of power during an upgrade can make a firewall unusable.

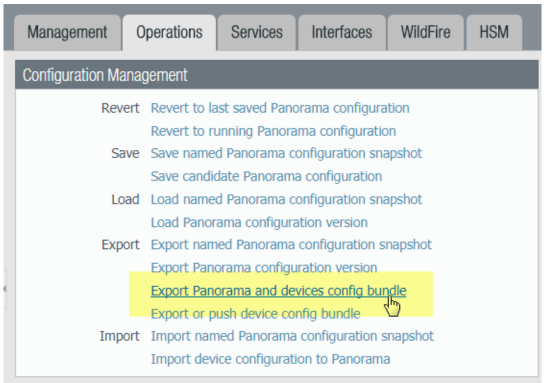
STEP 1 | After upgrading Panorama, commit and push the configuration to the firewalls you are planning to upgrade.

The PAN-OS 9.1 release introduces universally unique identifiers (UUIDs) for policy rules. If you manage firewall policy from Panorama, these UUIDs are generated on Panorama and therefore must be pushed from Panorama. If you do not push the configuration from Panorama prior to upgrading the firewalls, the firewall upgrade will not succeed because it will not have the UUIDs.

STEP 2 | 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. From the Panorama web interface, select **Panorama** > **Setup** > **Operations** and click **Export Panorama and devices config bundle** to generate and export the latest configuration backup of Panorama and of each managed appliance.



Configuration Management

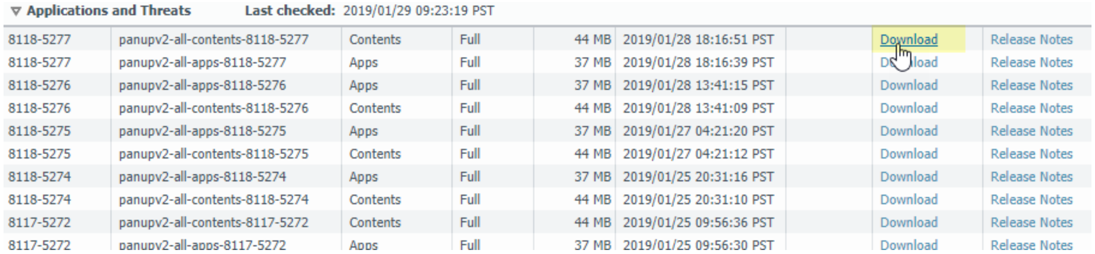
| | |
|---|---|
| Revert | Revert to last saved Panorama configuration |
| | Revert to running Panorama configuration |
| Save | Save named Panorama configuration snapshot |
| | Save candidate Panorama configuration |
| Load | Load named Panorama configuration snapshot |
| | Load Panorama configuration version |
| Export | Export named Panorama configuration snapshot |
| | Export Panorama configuration version |
| | Export Panorama and devices config bundle |
| | Export or push device config bundle |
| Import | Import named Panorama configuration snapshot |
| | Import device configuration to Panorama |

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 3 | Update the content release version on the firewalls you plan to upgrade.

Refer to the Release Notes for the minimum content release version required for PAN-OS 9.1. Make sure to follow the Best Practices for Application and Threat Updates when deploying content updates to Panorama and managed firewalls.

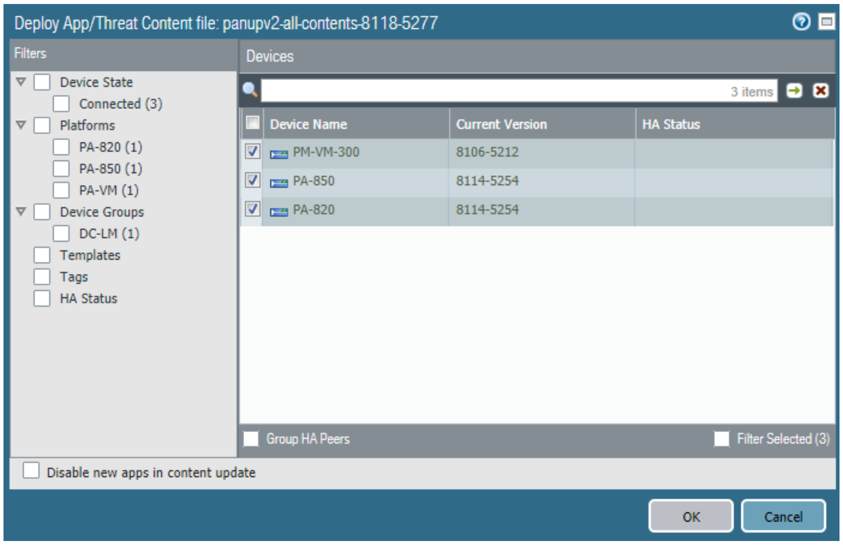
1. Select **Panorama** > **Device Deployment** > **Dynamic Updates** and **Check Now** for the latest updates. If an update is available, the Action column displays a **Download** link.



▽ **Applications and Threats** **Last checked:** 2019/01/29 09:23:19 PST

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 8118-5277 | panupv2-all-contents-8118-5277 | Contents | Full | 44 MB | 2019/01/28 18:16:51 PST | | Download | Release Notes |
| 8118-5277 | panupv2-all-apps-8118-5277 | Apps | Full | 37 MB | 2019/01/28 18:16:39 PST | | Download | Release Notes |
| 8118-5276 | panupv2-all-apps-8118-5276 | Apps | Full | 37 MB | 2019/01/28 13:41:15 PST | | Download | Release Notes |
| 8118-5276 | panupv2-all-contents-8118-5276 | Contents | Full | 44 MB | 2019/01/28 13:41:09 PST | | Download | Release Notes |
| 8118-5275 | panupv2-all-apps-8118-5275 | Apps | Full | 37 MB | 2019/01/27 04:21:20 PST | | Download | Release Notes |
| 8118-5275 | panupv2-all-contents-8118-5275 | Contents | Full | 44 MB | 2019/01/27 04:21:12 PST | | Download | Release Notes |
| 8118-5274 | panupv2-all-apps-8118-5274 | Apps | Full | 37 MB | 2019/01/25 20:31:16 PST | | Download | Release Notes |
| 8118-5274 | panupv2-all-contents-8118-5274 | Contents | Full | 44 MB | 2019/01/25 20:31:10 PST | | Download | Release Notes |
| 8117-5272 | panupv2-all-contents-8117-5272 | Contents | Full | 44 MB | 2019/01/25 09:56:36 PST | | Download | Release Notes |
| 8117-5272 | panupv2-all-apps-8117-5272 | Apps | Full | 37 MB | 2019/01/25 09:56:30 PST | | Download | Release Notes |

2. If not already installed, **Download** the latest content release version.
3. Click **Install**, select the firewalls on which you want to install the update, and click **OK**. If you are upgrading HA firewalls, you must update content on both peers.



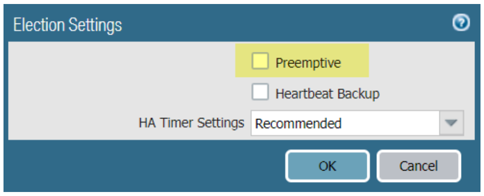
Deploy App/Threat Content file: panupv2-all-contents-8118-5277

| □ | Device Name | Current Version | HA Status |
|---|---|---|---|
| ☑ | PM-VM-300 | 8106-5212 | |
| ☑ | PA-850 | 8114-5254 | |
| ☑ | PA-820 | 8114-5254 | |

*By default, you can upload a maximum of two software or content updates of each type to a Panorama appliance and if you download a third update of the same type, Panorama will delete the update for the earliest version of that type. If you need to upload more than two software updates or content updates of a single type, use the* **`setmax-num-images count <number>`** *CLI command to increase the maximum.*

STEP 4 | (HA firewall upgrades only) If you will be upgrading firewalls that are part of an HA pair, disable preemption. You need only disable this setting on one firewall in each HA pair.

1. Select **Device** > **High Availability** and edit the **Election Settings**.
2. If enabled, disable (clear) the **Preemptive** setting and click **OK**.



Election Settings

□ Preemptive

□ Heartbeat Backup

HA Timer Settings: Recommended

3. **Commit** your change. Make sure the commit is successful before you proceed with the upgrade.

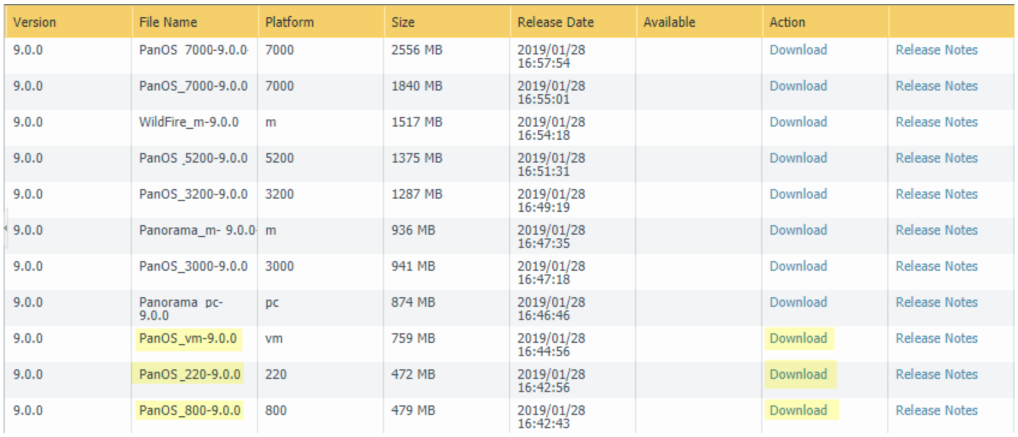
## STEP 5 | Determine the Upgrade Path to PAN-OS 9.1

You cannot skip installation of any feature release versions in the path from the currently running PAN-OS version to PAN-OS 9.1.0. 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.

*If upgrading more than one firewall, streamline the process by determining upgrade paths for all firewalls before you start downloading images.*

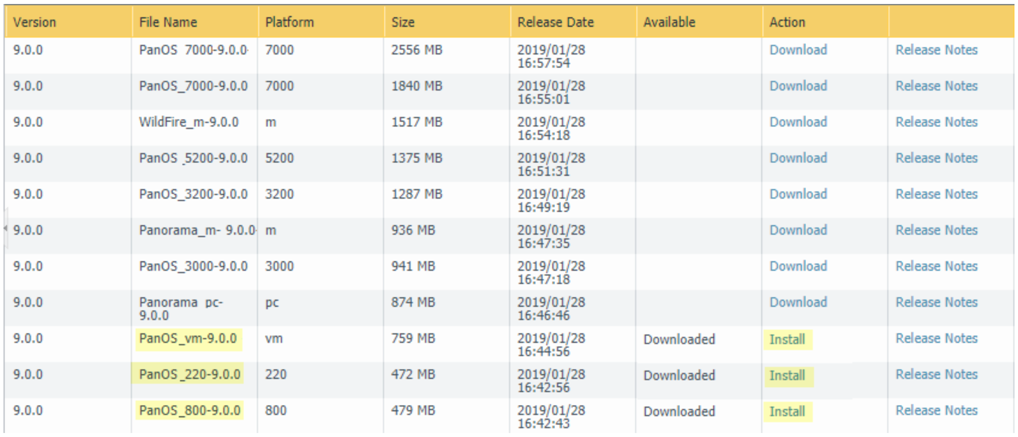
STEP 6 | Download the target PAN-OS 9.1 release image.

1. Select **Panorama** > **Device Deployment** > **Software** and **Check Now** for the latest release versions.
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 model (or firewall series) that you intend to upgrade.



| Version | File Name | Platform | Size | Release Date | Available | Action | |
|---|---|---|---|---|---|---|---|
| 9.0.0 | PanOS 7000-9.0.0 | 7000 | 2556 MB | 2019/01/28 16:57:54 | | Download | Release Notes |
| 9.0.0 | PanOS_7000-9.0.0 | 7000 | 1840 MB | 2019/01/28 16:55:01 | | Download | Release Notes |
| 9.0.0 | WildFire_m-9.0.0 | m | 1517 MB | 2019/01/28 16:54:18 | | Download | Release Notes |
| 9.0.0 | PanOS 5200-9.0.0 | 5200 | 1375 MB | 2019/01/28 16:51:31 | | Download | Release Notes |
| 9.0.0 | PanOS_3200-9.0.0 | 3200 | 1287 MB | 2019/01/28 16:49:19 | | Download | Release Notes |
| 9.0.0 | Panorama_m- 9.0.0 | m | 936 MB | 2019/01/28 16:47:35 | | Download | Release Notes |
| 9.0.0 | PanOS_3000-9.0.0 | 3000 | 941 MB | 2019/01/28 16:47:18 | | Download | Release Notes |
| 9.0.0 | Panorama pc-9.0.0 | pc | 874 MB | 2019/01/28 16:46:46 | | Download | Release Notes |
| 9.0.0 | PanOS_vm-9.0.0 | vm | 759 MB | 2019/01/28 16:44:56 | | Download | Release Notes |
| 9.0.0 | PanOS_220-9.0.0 | 220 | 472 MB | 2019/01/28 16:42:56 | | Download | Release Notes |
| 9.0.0 | PanOS_800-9.0.0 | 800 | 479 MB | 2019/01/28 16:42:43 | | Download | Release Notes |

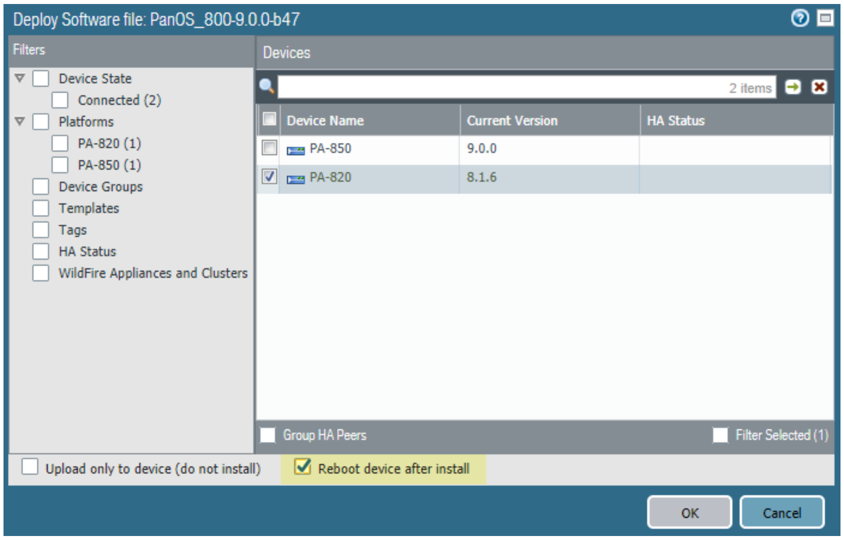
For example, to upgrade your PA-220, PA-820, and VM-300 firewalls to PAN-OS 9.1.0, download the `PanOS_220-9.1.0`, `PanOS_vm-9.1.0`, and `PanOS_800-9.1.0` images. After you successfully download an image, the Action column changes to **Install** for that image.



| Version | File Name | Platform | Size | Release Date | Available | Action | |
|---|---|---|---|---|---|---|---|
| 9.0.0 | PanOS 7000-9.0.0 | 7000 | 2556 MB | 2019/01/28 16:57:54 | | Download | Release Notes |
| 9.0.0 | PanOS_7000-9.0.0 | 7000 | 1840 MB | 2019/01/28 16:55:01 | | Download | Release Notes |
| 9.0.0 | WildFire_m-9.0.0 | m | 1517 MB | 2019/01/28 16:54:18 | | Download | Release Notes |
| 9.0.0 | PanOS 5200-9.0.0 | 5200 | 1375 MB | 2019/01/28 16:51:31 | | Download | Release Notes |
| 9.0.0 | PanOS_3200-9.0.0 | 3200 | 1287 MB | 2019/01/28 16:49:19 | | Download | Release Notes |
| 9.0.0 | Panorama_m- 9.0.0 | m | 936 MB | 2019/01/28 16:47:35 | | Download | Release Notes |
| 9.0.0 | PanOS_3000-9.0.0 | 3000 | 941 MB | 2019/01/28 16:47:18 | | Download | Release Notes |
| 9.0.0 | Panorama pc-9.0.0 | pc | 874 MB | 2019/01/28 16:46:46 | | Download | Release Notes |
| 9.0.0 | PanOS_vm-9.0.0 | vm | 759 MB | 2019/01/28 16:44:56 | Downloaded | Install | Release Notes |
| 9.0.0 | PanOS_220-9.0.0 | 220 | 472 MB | 2019/01/28 16:42:56 | Downloaded | Install | Release Notes |
| 9.0.0 | PanOS_800-9.0.0 | 800 | 479 MB | 2019/01/28 16:42:43 | Downloaded | Install | Release Notes |

STEP 7 | Install the PAN-OS 9.1 software update on the firewalls.

1. Click **Install** in the Action column that corresponds to the firewall models you want to upgrade. For example, if you want to upgrade your PA-820 firewalls, click **Install** in the row that corresponds to PanOS_800-9.1.0.
2. In the Deploy Software file dialog, select all firewalls that you want to upgrade. To reduce downtime, select only one peer in each HA pair. For active/passive pairs, select the passive peer; for active/active pairs, select the active-secondary peer.
3. (HA firewall upgrades only) Make sure **Group HA Peers** is not selected.
4. Select **Reboot device after install**.
5. To begin the upgrade, click **OK**.



Deploy Software file: PanOS_800-9.0.0-b47

Filters

- ▽ □ Device State
  - □ Connected (2)
- ▽ □ Platforms
  - □ PA-820 (1)
  - □ PA-850 (1)
- □ Device Groups
- □ Templates
- □ Tags
- □ HA Status
- □ WildFire Appliances and Clusters

Devices (2 items)

| □ | Device Name | Current Version | HA Status |
|---|---|---|---|
| □ | PA-850 | 9.0.0 | |
| ☑ | PA-820 | 8.1.6 | |

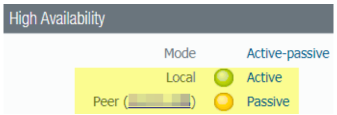
□ Group HA Peers    □ Filter Selected (1)

□ Upload only to device (do not install)    ☑ Reboot device after install

6. 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, select **Device** > **Setup** > **Operations** and **Reboot Device**.
7. After the firewalls finish rebooting, select **Panorama** > **Managed Devices** and verify the Software Version is 9.1.0 for the firewalls you upgraded. Also verify that the HA status of any passive firewalls you upgraded is still passive.

## STEP 8 | (HA firewall upgrades only) Upgrade the second HA peer in each HA pair.

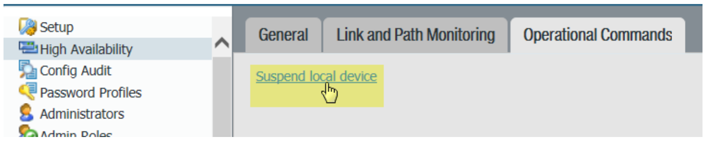
1. (Active/passive upgrades only) Suspend the active device in each active/passive pair you are upgrading.
   1. Switch context to the active firewall.
   2. In the High Availability widget on the **Dashboard**, verify that **Local** firewall state is **Active** and the **Peer** is **Passive**).

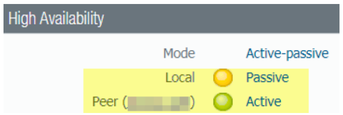
      High Availability

      | | | |
      |---|---|---|
      | Mode | | Active-passive |
      | Local | ● | Active |
      | Peer ([redacted]) | ● | Passive |

   3. Select **Device** > **High Availability** > **Operational Commands** > **Suspend local device**.

   4. Go back to the High Availability widget on the **Dashboard** and verify that **Local** changed to **Passive** and **Peer** changed to **Active**.

      High Availability

      | | | |
      |---|---|---|
      | Mode | | Active-passive |
      | Local | ● | Passive |
      | Peer ([redacted]) | ● | Active |

2. Go back to the Panorama context and select **Panorama** > **Device Deployment** > **Software**.
3. Click **Install** in the Action column that corresponds to the firewall models of the HA pairs you are upgrading.
4. In the Deploy Software file dialog, select all firewalls that you want to upgrade. This time, select only the peers of the HA firewalls you just upgraded.
5. Make sure **Group HA Peers** is not selected.

6. Select **Reboot device after install**.
7. To begin the upgrade, click **OK**.
8. 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, select **Device** > **Setup** > **Operations** and **Reboot Device**.
9. (Active/passive upgrades only) From the CLI of the peer you just upgraded, run the following command to make the firewall functional again:

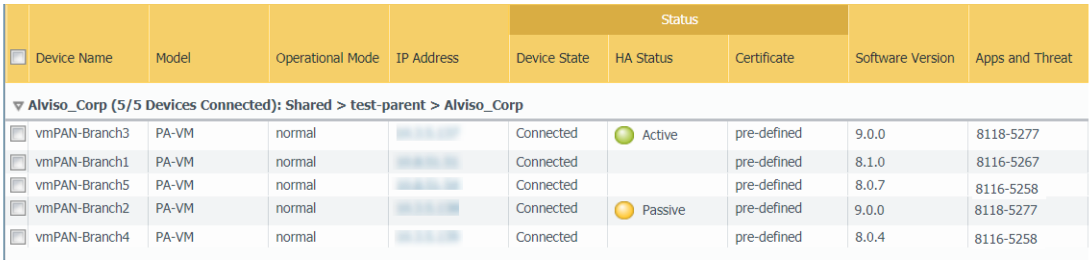
```
request high-availability state functional
```

STEP 9 | 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.

   For HA firewalls, you can also verify that the HA Status of each peer is as expected.

   *If your HA firewalls have local policy rules configured, upon upgrade to PAN-OS 9.1, each peer independently assigns UUIDs for each rule. Because of this, the peers will show as out of sync until you sync the configuration (Dashboard > Widgets > System > High Availability > Sync to peer).*



| □ | | | | | Status | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Device Name | Model | Operational Mode | IP Address | Device State | HA Status | Certificate | Software Version | Apps and Threat |
| ▿ Alviso_Corp (5/5 Devices Connected): Shared > test-parent > Alviso_Corp | | | | | | | | | |
| □ | vmPAN-Branch3 | PA-VM | normal | [redacted] | Connected | ● Active | pre-defined | 9.0.0 | 8118-5277 |
| □ | vmPAN-Branch1 | PA-VM | normal | [redacted] | Connected | | pre-defined | 8.1.0 | 8116-5267 |
| □ | vmPAN-Branch5 | PA-VM | normal | [redacted] | Connected | | pre-defined | 8.0.7 | 8116-5258 |
| □ | vmPAN-Branch2 | PA-VM | normal | [redacted] | Connected | ● Passive | pre-defined | 9.0.0 | 8118-5277 |
| □ | vmPAN-Branch4 | PA-VM | normal | [redacted] | Connected | | pre-defined | 8.0.4 | 8116-5258 |

STEP 10 | (HA firewall upgrades only) If you disabled preemption on one of your HA firewalls before you upgraded, then edit the **Election Settings** (**Device** > **High Availability**) and re-enable the **Preemptive** setting for that firewall and then **Commit** the change.

## Upgrade a Standalone Firewall to PAN-OS 9.1

Review the PAN-OS 9.1 Release Notes and then use the following procedure to upgrade a firewall that is not in an HA configuration to PAN-OS 9.1.

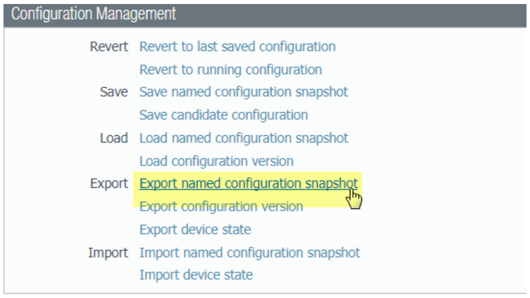
*If your firewalls are configured to forward samples to a WildFire appliance for analysis, you must* upgrade the WildFire appliance *before upgrading the forwarding firewalls.*

*To avoid impacting traffic, plan to upgrade within the outage window. Ensure the firewall is connected to a reliable power source. A loss of power during an upgrade can make the firewall unusable.*

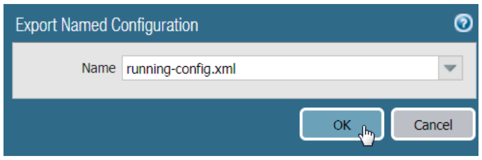
STEP 1 | Save a backup of the current configuration file.

*Although the firewall automatically creates a configuration backup, it is a best practice to create and externally store a backup before you upgrade.*

1. Select **Device** > **Setup** > **Operations** and click **Export named configuration snapshot**.


Configuration Management
Revert
Revert to last saved configuration
Revert to running configuration
Save
Save named configuration snapshot
Save candidate configuration
Load
Load named configuration snapshot
Load configuration version
Export
Export named configuration snapshot
Export configuration version
Export device state
Import
Import named configuration snapshot
Import device state

2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file.



Name: running-config.xml

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.

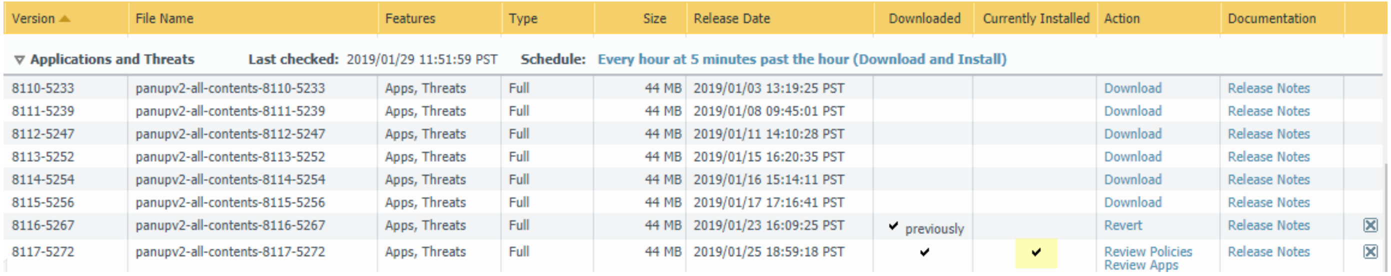
STEP 2 | If you have enabled User-ID, after you upgrade, the firewall clears the current IP address-to-username and group mappings so that they can be repopulated with the attributes from the User-ID sources. To estimate the time required for your environment to repopulate the mappings, run the following CLI commands on the firewall.

- For IP address-to-username mappings:
  - `show user user-id-agent state all`
  - `show user server-monitor state all`
- For group mappings: `show user group-mapping statistics`

STEP 3 | Ensure that the firewall is running the latest content release version.

Refer to the Release Notes for the minimum content release version you must install for a PAN-OS 9.1 release. Make sure to follow the Best Practices for Application and Threat Updates.

1. Select **Device** > **Dynamic Updates** and see which **Applications** or **Applications and Threats** content release version is Currently Installed.



▽ Applications and Threats   Last checked: 2019/01/29 11:51:59 PST   Schedule: Every hour at 5 minutes past the hour (Download and Install)

| Version ▲ | File Name | Features | Type | Size | Release Date | Downloaded | Currently Installed | Action | Documentation | |
|---|---|---|---|---|---|---|---|---|---|---|
| 8110-5233 | panupv2-all-contents-8110-5233 | Apps, Threats | Full | 44 MB | 2019/01/03 13:19:25 PST | | | Download | Release Notes | |
| 8111-5239 | panupv2-all-contents-8111-5239 | Apps, Threats | Full | 44 MB | 2019/01/08 09:45:01 PST | | | Download | Release Notes | |
| 8112-5247 | panupv2-all-contents-8112-5247 | Apps, Threats | Full | 44 MB | 2019/01/11 14:10:28 PST | | | Download | Release Notes | |
| 8113-5252 | panupv2-all-contents-8113-5252 | Apps, Threats | Full | 44 MB | 2019/01/15 16:20:35 PST | | | Download | Release Notes | |
| 8114-5254 | panupv2-all-contents-8114-5254 | Apps, Threats | Full | 44 MB | 2019/01/16 15:14:11 PST | | | Download | Release Notes | |
| 8115-5256 | panupv2-all-contents-8115-5256 | Apps, Threats | Full | 44 MB | 2019/01/17 17:16:41 PST | | | Download | Release Notes | |
| 8116-5267 | panupv2-all-contents-8116-5267 | Apps, Threats | Full | 44 MB | 2019/01/23 16:09:25 PST | ✓ previously | | Revert | Release Notes | ☒ |
| 8117-5272 | panupv2-all-contents-8117-5272 | Apps, Threats | Full | 44 MB | 2019/01/25 18:59:18 PST | ✓ | ✓ | Review Policies<br>Review Apps | Release Notes | ☒ |

2. If the firewall is not running the minimum required content release version or a later version required for PAN-OS 9.1, **Check Now** to retrieve a list of available updates.
3. Locate and **Download** the desired content release version.

   After you successfully download a content update file, the link in the Action column changes from **Download** to **Install** for that content release version.
4. **Install** the update.

STEP 4 | Determine the Upgrade Path to PAN-OS 9.1

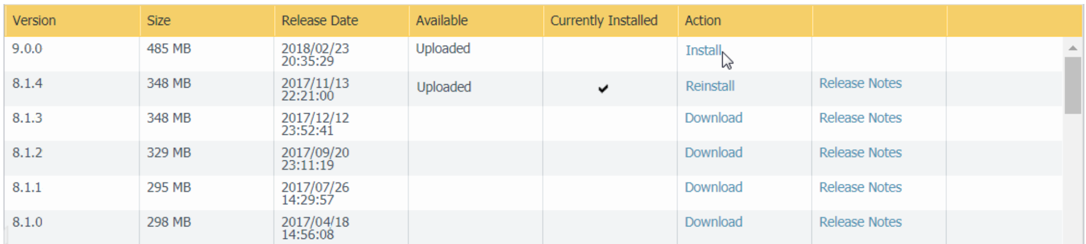
You cannot skip installation of any feature release versions in the path from the currently running PAN-OS version to PAN-OS 9.1.0.

*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 5 | Upgrade to PAN-OS 9.1.

*If your firewall does not have internet access from the management port, you can download the software image from the Palo Alto Networks Customer Support Portal and then manually Upload it to your firewall.*

1. Select **Device** > **Software** and click **Check Now** to display the latest PAN-OS updates.
2. Locate and **Download** PAN-OS 9.1.0.
3. After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image.



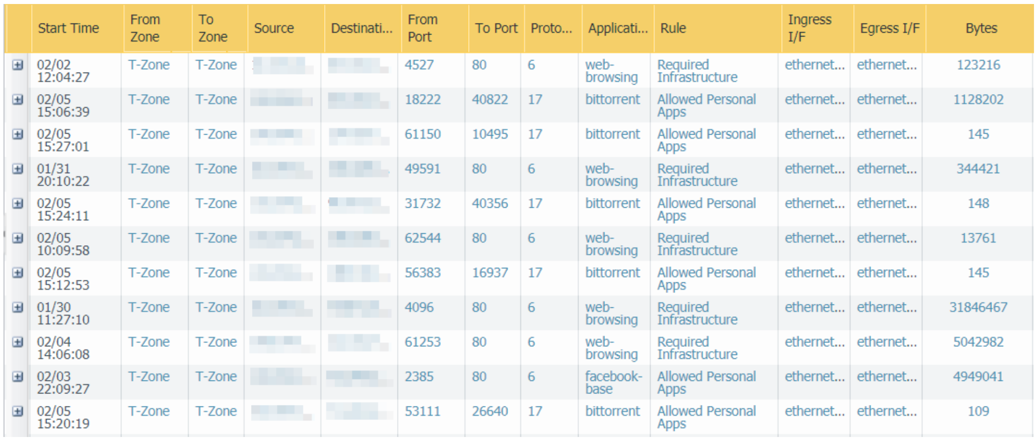
| Version | Size | Release Date | Available | Currently Installed | Action | | |
|---|---|---|---|---|---|---|---|
| 9.0.0 | 485 MB | 2018/02/23 20:35:29 | Uploaded | | Install | | |
| 8.1.4 | 348 MB | 2017/11/13 22:21:00 | Uploaded | ✓ | Reinstall | Release Notes | |
| 8.1.3 | 348 MB | 2017/12/12 23:52:41 | | | Download | Release Notes | |
| 8.1.2 | 329 MB | 2017/09/20 23:11:19 | | | Download | Release Notes | |
| 8.1.1 | 295 MB | 2017/07/26 14:29:57 | | | Download | Release Notes | |
| 8.1.0 | 298 MB | 2017/04/18 14:56:08 | | | Download | Release Notes | |

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, select **Device** > **Setup** > **Operations** and click **Reboot Device**.

   *At this point, the firewall clears the User-ID mappings, then connects to the User-ID sources to repopulate the mappings.*
5. If you have enabled User-ID, use the following CLI commands to verify that the firewall has repopulated the IP address-to-username and group mappings before allowing traffic.
   - **`show user ip-user-mapping all`**
   - **`show user group list`**

STEP 6 | Verify that the firewall is passing traffic.

Select **Monitor** > **Session Browser** and verify that you are seeing new sessions.



| | Start Time | From Zone | To Zone | Source | Destinati... | From Port | To Port | Proto... | Applicati... | Rule | Ingress I/F | Egress I/F | Bytes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ⊞ | 02/02 12:04:27 | T-Zone | T-Zone | [redacted] | [redacted] | 4527 | 80 | 6 | web-browsing | Required Infrastructure | ethernet... | ethernet... | 123216 |
| ⊞ | 02/05 15:06:39 | T-Zone | T-Zone | [redacted] | [redacted] | 18222 | 40822 | 17 | bittorrent | Allowed Personal Apps | ethernet... | ethernet... | 1128202 |
| ⊞ | 02/05 15:27:01 | T-Zone | T-Zone | [redacted] | [redacted] | 61150 | 10495 | 17 | bittorrent | Allowed Personal Apps | ethernet... | ethernet... | 145 |
| ⊞ | 01/31 20:10:22 | T-Zone | T-Zone | [redacted] | [redacted] | 49591 | 80 | 6 | web-browsing | Required Infrastructure | ethernet... | ethernet... | 344421 |
| ⊞ | 02/05 15:24:11 | T-Zone | T-Zone | [redacted] | [redacted] | 31732 | 40356 | 17 | bittorrent | Allowed Personal Apps | ethernet... | ethernet... | 148 |
| ⊞ | 02/05 10:09:58 | T-Zone | T-Zone | [redacted] | [redacted] | 62544 | 80 | 6 | web-browsing | Required Infrastructure | ethernet... | ethernet... | 13761 |
| ⊞ | 02/05 15:12:53 | T-Zone | T-Zone | [redacted] | [redacted] | 56383 | 16937 | 17 | bittorrent | Allowed Personal Apps | ethernet... | ethernet... | 145 |
| ⊞ | 01/30 11:27:10 | T-Zone | T-Zone | [redacted] | [redacted] | 4096 | 80 | 6 | web-browsing | Required Infrastructure | ethernet... | ethernet... | 31846467 |
| ⊞ | 02/04 14:06:08 | T-Zone | T-Zone | [redacted] | [redacted] | 61253 | 80 | 6 | web-browsing | Required Infrastructure | ethernet... | ethernet... | 5042982 |
| ⊞ | 02/03 22:09:27 | T-Zone | T-Zone | [redacted] | [redacted] | 2385 | 80 | 6 | facebook-base | Allowed Personal Apps | ethernet... | ethernet... | 4949041 |
| ⊞ | 02/05 15:20:19 | T-Zone | T-Zone | [redacted] | [redacted] | 53111 | 26640 | 17 | bittorrent | Allowed Personal Apps | ethernet... | ethernet... | 109 |

## Upgrade an HA Firewall Pair to PAN-OS 9.1

Review the PAN-OS 9.1 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.

To avoid downtime when upgrading firewalls that are in a high availability (HA) configuration, update one HA peer at a time: For active/active firewalls, it doesn't matter which peer you upgrade first (though for simplicity, this procedure shows you how to upgrade the active-secondary peer first). For active/passive firewalls, you must upgrade the passive peer first, suspend the active peer (fail over), update the active peer, and then return that peer to a functional state (fail back). To prevent failover during the upgrade of the HA peers, you must make sure preemption is disabled before proceeding with the upgrade. You only need to disable preemption on one peer in the pair.

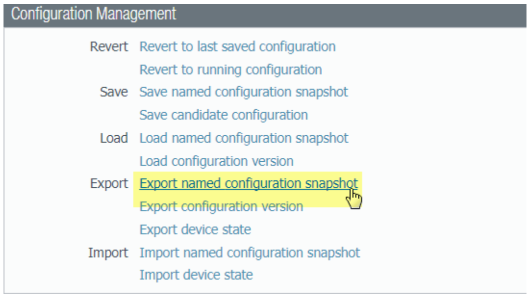
*To avoid impacting traffic, plan to upgrade within the outage window. Ensure the firewalls are connected to a reliable power source. A loss of power during an upgrade can make firewalls unusable.*

STEP 1 | Save a backup of the current configuration file.

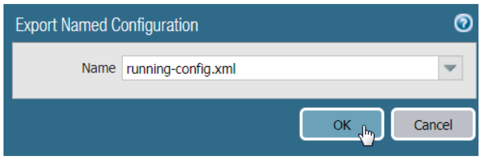
*Although the firewall automatically creates a backup of the configuration, it is a best practice to create and externally store a backup before you upgrade.*

Perform these steps on each firewall in the pair:

1. Select **Device** > **Setup** > **Operations** and click **Export named configuration snapshot**.


Configuration Management
Revert
Revert to last saved configuration
Revert to running configuration
Save
Save named configuration snapshot
Save candidate configuration
Load
Load named configuration snapshot
Load configuration version
Export
Export named configuration snapshot
Export configuration version
Export device state
Import
Import named configuration snapshot
Import device state

2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file.



Name: running-config.xml

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.

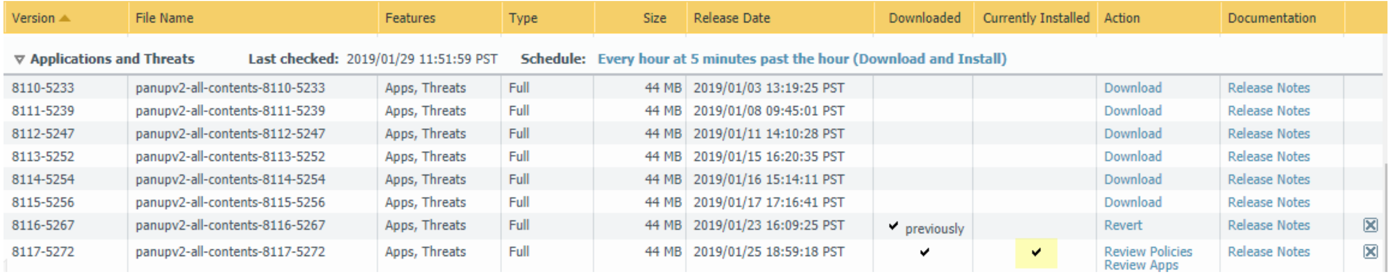
STEP 2 | If you have enabled User-ID, after you upgrade, the firewall clears the current IP address-to-username and group mappings so that they can be repopulated with the attributes from the User-ID sources. To estimate the time required for your environment to repopulate the mappings, run the following CLI commands on the firewall.

- For IP address-to-username mappings:
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- For group mappings: **`show user group-mapping statistics`**

STEP 3 | Ensure that each firewall in the HA pair is running the latest content release version.

Refer to the release notes for the minimum content release version you must install for a PAN-OS 9.1 release. Make sure to follow the Best Practices for Application and Threat Updates.

1. Select **Device** > **Dynamic Updates** and check which **Applications** or **Applications and Threats** to determine which update is Currently Installed.



▽ Applications and Threats **Last checked:** 2019/01/29 11:51:59 PST **Schedule:** Every hour at 5 minutes past the hour (Download and Install)

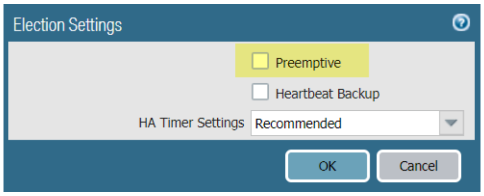
| Version ▲ | File Name | Features | Type | Size | Release Date | Downloaded | Currently Installed | Action | Documentation | |
|---|---|---|---|---|---|---|---|---|---|---|
| 8110-5233 | panupv2-all-contents-8110-5233 | Apps, Threats | Full | 44 MB | 2019/01/03 13:19:25 PST | | | Download | Release Notes | |
| 8111-5239 | panupv2-all-contents-8111-5239 | Apps, Threats | Full | 44 MB | 2019/01/08 09:45:01 PST | | | Download | Release Notes | |
| 8112-5247 | panupv2-all-contents-8112-5247 | Apps, Threats | Full | 44 MB | 2019/01/11 14:10:28 PST | | | Download | Release Notes | |
| 8113-5252 | panupv2-all-contents-8113-5252 | Apps, Threats | Full | 44 MB | 2019/01/15 16:20:35 PST | | | Download | Release Notes | |
| 8114-5254 | panupv2-all-contents-8114-5254 | Apps, Threats | Full | 44 MB | 2019/01/16 15:14:11 PST | | | Download | Release Notes | |
| 8115-5256 | panupv2-all-contents-8115-5256 | Apps, Threats | Full | 44 MB | 2019/01/17 17:16:41 PST | | | Download | Release Notes | |
| 8116-5267 | panupv2-all-contents-8116-5267 | Apps, Threats | Full | 44 MB | 2019/01/23 16:09:25 PST | ✓ previously | | Revert | Release Notes | ☒ |
| 8117-5272 | panupv2-all-contents-8117-5272 | Apps, Threats | Full | 44 MB | 2019/01/25 18:59:18 PST | ✓ | ✓ | Review Policies<br>Review Apps | Release Notes | ☒ |

2. If the firewalls are not running the minimum required content release version or a later version required for PAN-OS 9.1, **Check Now** to retrieve a list of available updates.
3. Locate and **Download** the desired content release version.

   After you successfully download a content update file, the link in the Action column changes from **Download** to **Install** for that content release version.
4. **Install** the update. You must install the update on both peers.

STEP 4 | Disable preemption on the first peer in each pair. You only need to disable this setting on one firewall in the HA pair but ensure that the commit is successful before you proceed with the upgrade.

1. Select **Device** > **High Availability** and edit the **Election Settings**.
2. If enabled, disable (clear) the **Preemptive** setting and click **OK**.



☐ Preemptive
☐ Heartbeat Backup
HA Timer Settings: Recommended

3. **Commit** the change.

## STEP 5 | Determine the Upgrade Path to PAN-OS 9.1

You cannot skip installation of any feature release versions in the path from the currently running PAN-OS version to PAN-OS 9.1.0.

*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 6 | Install PAN-OS 9.1 on the first peer.

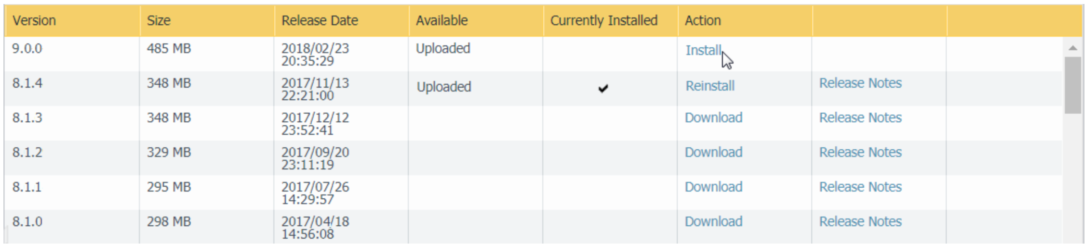
To minimize downtime in an active/passive configuration, upgrade the passive peer first. For an active/active configuration, upgrade the secondary peer first. As a best practice, if you are using an active/active configuration, we recommend upgrading both peers during the same maintenance window.

*If you want to test that HA is functioning properly before the upgrade, consider upgrading the active peer in an active/passive configuration first to ensure that failover occurs without incident.*

1. On the first peer, select **Device** > **Software** and click **Check Now** for the latest updates.
2. Locate and **Download** PAN-OS 9.1.0.

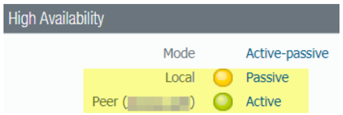
    *If your firewall does not have internet access from the management port, you can download the software image from the Palo Alto Networks Support Portal and then manually Upload it to your firewall.*

3. After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image.



| Version | Size | Release Date | Available | Currently Installed | Action | | |
|---|---|---|---|---|---|---|---|
| 9.0.0 | 485 MB | 2018/02/23 20:35:29 | Uploaded | | Install | | |
| 8.1.4 | 348 MB | 2017/11/13 22:21:00 | Uploaded | ✓ | Reinstall | Release Notes | |
| 8.1.3 | 348 MB | 2017/12/12 23:52:41 | | | Download | Release Notes | |
| 8.1.2 | 329 MB | 2017/09/20 23:11:19 | | | Download | Release Notes | |
| 8.1.1 | 295 MB | 2017/07/26 14:29:57 | | | Download | Release Notes | |
| 8.1.0 | 298 MB | 2017/04/18 14:56:08 | | | Download | Release Notes | |

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, select **Device** > **Setup** > **Operations** and **Reboot Device**.
5. After the device finishes rebooting, view the High Availability widget on the **Dashboard** and verify that the device you just upgraded is still the passive or active-secondary peer in the HA configuration.



High Availability

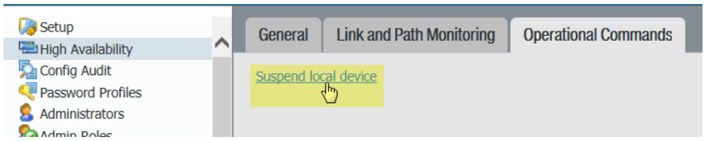
Mode Active-passive

Local ● Passive

Peer ([redacted]) ● Active

## STEP 7 | Install PAN-OS 9.1 on the second peer.

1. (Active/passive configurations only) Suspend the active peer so that HA fails over to the peer you just upgraded.
    1. On the active peer, select **Device** > **High Availability** > **Operational Commands** and click **Suspend local device**.



   2. View the High Availability widget on the **Dashboard** and verify that the state changes to **Passive**.
   3. On the other peer, verify that it is active and is passing traffic (**Monitor** > **Session Browser**).
2. On the second peer, select **Device** > **Software** and click **Check Now** for the latest updates.
3. Locate and **Download** PAN-OS 9.1.0.
4. After you download the image, **Install** it.
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, select **Device** > **Setup** > **Operations** and **Reboot Device**.
6. (Active/passive configurations only) From the CLI of the peer you just upgraded, run the following command to make the firewall functional again:

```
request high-availability state functional
```

*If your HA firewalls have local policy rules configured, upon upgrade to PAN-OS 9.1, each peer independently assigns UUIDs for each rule. Because of this, the peers will show as out of sync until you sync the configuration (Dashboard > Widgets > System > High Availability > Sync to peer).*

STEP 8 | Verify that both peers 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.

STEP 9 | If you disabled preemption prior to the upgrade, re-enable it now.

1. Select **Device** > **High Availability** and edit the **Election Settings**.
2. Select **Preemptive** and click **OK**.
3. **Commit** the change.

# Downgrade from PAN-OS 9.1

The way you downgrade a firewall from PAN-OS 9.1 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 8.1.2 to 8.0.13 or from 8.0.6 to 7.1.9) or downgrading to a maintenance release version within the same feature release (where the third digit in the release version changes, for example, from 8.1.2 to 8.1.0). 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 9.1 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 9.1

*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 9.0.0 to 8.1.3), not to downgrades to maintenance releases within the same feature release version (for example, 8.1.3 to 8.1.1).*

*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 8.1.6 to 8.1.4 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.

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. **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 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. **Check Now** (**Device** > **Software**) for available images.
2. Locate the version to which you want to downgrade. If the image is not already downloaded, then **Download** it.
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. Therefore, it is important to back up your current configuration so you can restore those changes when you return to the newer feature release.

Use the following procedure to 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. **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 downgrade.

STEP 2 | Install the previous feature release image.

*Autosave versions are created when you upgrade to a new release.*

1. **Check Now** (**Device** > **Software**) for available images.
2. Locate the image to which you want to downgrade. If the image is not already downloaded, then **Download** it.
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 9.1 and are downgrading to PAN-OS 9.0.4, select `autosave-9.0.4`.
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 9.1

After you uninstall the PAN-OS 9.1 Windows-based User-ID agent, perform the following steps before you install an earlier agent release.

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.

# SD-WAN Features

# Secure SD-WAN

Software-Defined Wide Area Network (SD-WAN) is a technology that allows you to use multiple internet and private services to create an intelligent and dynamic WAN, which helps lower costs and maximize application quality and usability. Beginning with PAN-OS® 9.1, Palo Alto Networks offers strong security with an SD-WAN subscription in a single management system. Instead of using costly and time-consuming MPLS with components such as routers, firewalls, WAN link controllers, and WAN optimizers to connect your WAN to the internet, SD-WAN on a Palo Alto Networks® firewall allows you to use less expensive internet services and fewer pieces of equipment. You don't need to purchase and maintain other WAN components.

You install the SD-WAN plugin on the Panorama™ management server, so that you get the security features of a PAN-OS management and firewall, and SD-WAN functionality from a single vendor. The SD-WAN subscription supports dynamic, intelligent link selection based on applications and services and the conditions of links that each application or service is allowed to use. The path health monitoring for each link includes latency, jitter, and packet loss. Granular application and service controls allow you to prioritize applications based on whether the application is mission-critical, latency-sensitive, or meets certain health criteria, for example. Dynamic path selection avoids brownout and node failure problems because sessions fail over to a better performing path in less than one second.

The SD-WAN subscription works with all PAN-OS security features, such as User-ID™ and App-ID™, to provide complete security control to branch offices. The App-ID capabilities identify applications (App-ID decoder, App-ID cache, and source/destination external dynamic list [EDL] IP address lists) for application-based control. You can deploy the firewall with Zero Trust segmentation of traffic. You can configure and manage SD-WAN centrally from the Panorama web interface or the Panorama REST API.

You may have cloud-based services and instead of having your internet traffic flow from branches to the hub to the cloud, you want the internet traffic to flow directly from branches to the cloud using a directly connected ISP. Such access from a branch to the internet is Direct Internet Access (DIA). You don't need to spend your hub bandwidth and money on internet traffic. The branch firewall is already doing security, so you don't need the hub firewall to enforce security on internet traffic. Use DIA on branches for SaaS, web browsing, or heavy-bandwidth applications that shouldn't be backhauled to a hub.

PA-220, PA-220R, PA-820, and PA-850 firewalls are supported as SD-WAN branch firewalls. PA-3200 Series, PA-5200 Series, VM-300, VM-500, and VM-700 firewalls are supported as SD-WAN hub firewalls. Each firewall (branch or hub) requires an SD-WAN subscription. Each Panorama requires the SD-WAN plugin.

STEP 1 | Read about SD-WAN to learn more about SD-WAN and the SD-WAN configuration elements.

STEP 2 | Plan your SD-WAN configuration. This includes planning the hub and branch firewall locations, link requirements, IP addresses and link bundles, as well as determining which applications will use SD-WAN and QoS optimization, and determining when and how you want links to fail over in the event the original link degrades or fails.

STEP 3 | Set up SD-WAN.

1. Install the SD-WAN plugin.
2. Set up Panorama and firewalls for SD-WAN by adding your SD-WAN firewalls as managed firewalls, as well as creating the template, template stacks, device groups, and zones required to push configuration changes from Panorama to your SD-WAN firewalls.

STEP 4 | Create your link tags to identify one or more physical links that you want applications and services to use in specific order during SD-WAN traffic distribution and failover protection.

STEP 5 | Configure an SD-WAN interface profile to define the characteristics of ISP connections and to specify the speed of links and how frequently the firewalls monitor the link.

STEP 6 | Configure a physical Ethernet interface for SD-WAN to enable SD-WAN functionality.

STEP 7 | Configure a virtual SD-WAN interface to specify one or more physical, SD-WAN-capable ethernet interfaces that go to the same destination.

STEP 8 | Create a path quality profile for each set of applications, application filters, application groups, service objects, and service group objects that has unique network health requirements. The health requriements are based on latency, jitter, and packet loss percentage.

STEP 9 | Create a traffic distribution profile to instruct the firewall how to select a new link in the event of link degradation to ensure users experience the best performance. The traffic distribution profile is applied to SD-WAN policy rules.

STEP 10 | Configure an SD-WAN policy rule to specify application(s) or service(s) and a traffic distribution profile to determine how the firewall selects the preferred path for incoming traffic.

STEP 11 | Add SD-WAN devices to Panorama. You can add a single managed firewall as an SD-WAN firewall or bulk import multiple managed firewalls.

STEP 12 | Create a VPN cluster to determine which branch firewalls communicate with which hub firewalls and create a secure connection between those branch and hub firewalls.

STEP 13 | Monitor your SD-WAN apps and links to troubleshoot and generate reports as needed.

# App-ID Features

- Streamlined Application-Based Policy
- Simplified Application Dependency Workflow

# Streamlined Application-Based Policy

You can now safely enable a broad set of applications with common attributes using a single policy rule (for example, you can allow your users broad access to web-based applications or safely enable all enterprise VoIP applications). Palo Alto Networks takes on the task of researching applications with common attributes and delivers this through tags in dynamic content updates. This:

- Minimizes errors and saves time.
- Helps you to create policies that automatically update to handle newly released applications.
- Simplifies the transition toward an App-ID based rule set using Policy Optimizer.

Your firewall can then use your tag-based application filter to dynamically enforce new and updated App-IDs, without requiring you to review or update policy rules whenever new applications are added. This reduces the chances that new or updated App-IDs will impact application availability or that a risky application is misclassified. You aren't required to know and assess every single application and can create policy rules based on the tag. For categories with higher risk, this also makes policy rules more precise as content updates keep the policy rules current.

If you choose to exclude applications from a specific tag, new content updates honor those exclusions. You can also use your own tags to define applications types based on your policy requirements.

Apply Tags to an Application Filter and Create Custom Application Tags provide detailed steps for using the new tags.

# Simplified Application Dependency Workflow

You now have simplified workflows to find and manage any application dependencies. These workflows allow you to see application dependencies when you create a new Security policy rule and when performing Commits. When a policy does not include all application dependencies, you can directly access the associated Security policy rule to add the required applications.

Using these workflows along with Policy Optimizer, you can now more easily identify, organize, and resolve application dependencies. You can take advantage of the new workflows by upgrading your Panorama management server to 9.1 and pushing rules to your firewalls. Resolve Application Dependencies provides detailed steps.

STEP 1 | Create a security policy rule.

STEP 2 | Specify the application that the rule will allow or block.

STEP 3 | Click **OK** and **Commit** your changes.

1. Review any Commit warnings in the **App Dependency** tab.
2. Select the **Rule** name to open the policy and add the dependencies.
3. Click **OK** and **Commit** your changes.

# *Panorama Features*

- Automatic Panorama Connection Recovery
- Next-Generation Firewalls for Zero Touch Provisioning

# Automatic Panorama Connection Recovery

Recovering isolated firewalls can be painful as it can result in unintended downtime and a loss in productivity. PAN-OS 9.1.0 introduces the ability for managed firewalls to check for connectivity to the Panorama™ management server and automatically revert to the last running configuration when the firewall is unable to communicate with Panorama. This helps you quickly resolve any configuration or connectivity issues without the need for manual intervention.

Automatic commit recovery allows you to configure the firewall to attempt a specified number of connectivity tests after you push a configuration from Panorama or commit a configuration change locally on the firewall. Additionally, the firewall checks connectivity to Panorama every hour to ensure consistent communication in the event unrelated network configuration changes have disrupted connectivity between the firewall and Panorama or if implications to a pushed committed configuration may have affected connectivity. If an hourly connectivity check fails, the firewall generates a system log to alert admins of potential configuration or network connectivity issues. Additionally, a system log is generated when you disable the setting, a connectivity test fails, or when a firewall configuration reverts to the last running configuration.

In high availability (HA) firewall configurations, each HA peer performs connectivity tests independently of each other, and HA config syncs may only occur after each HA successfully tests connectivity to Panorama and verifies their connection.

STEP 1 | Log in to the Panorama Web Interface.

STEP 2 | Select **Device** > **Setup** > **Management**.

STEP 3 | In the Template context drop-down, select the template or template stack that manages the devices for which you would like to configure the automated commit recovery parameters.

STEP 4 | Configure the automated commit recovery settings.

1. **Edit** (⚙) the Panorama Settings.
2. Verify that **Enable automated commit recovery** is enabled (checked).
3. Enter the **Number of attempts to check for Panorama connectivity**.
4. Enter the **Interval between retries**.
5. Click **OK** to save your configuration changes.

STEP 5 | Repeat Steps 3 and 4 for templates or template stacks as needed.

STEP 6 | Select **Commit** and **Commit and Push** your configuration changes.

# Next-Generation Firewalls for Zero Touch Provisioning

Zero Touch Provisioning (ZTP) is designed to simplify and automate the on-boarding of new firewalls to the Panorama™ management server. ZTP streamlines the initial firewall deployment process by allowing network administrators to ship managed firewalls directly to their branches and automatically add the firewall to the Panorama™ management server after the ZTP firewall successfully connects to the Palo Alto Networks ZTP service. This allows businesses to save on time and resources when deploying new firewalls at branch locations by removing the need for IT administrators to manually provision the new managed firewall. After successful on-boarding, Panorama provides the means to configure and manage your ZTP configuration and firewalls.

ZTP is supported on the following ZTP firewalls running PAN-OS 9.1.3 and later releases:

- PA-220-ZTP and PA-220R-ZTP
- PA-820-ZTP and PA-850-ZTP
- PA-3220-ZTP, PA-3250-ZTP, and PA-3260-ZTP

STEP 1 | Log in to the Panorama web interface as a superuser or Panorama administrator with access to Panorama plugins (**Panorama** > **Plugins**).

STEP 2 | Select **Panorama** > **Plugins** to **Download** and **Install** the most recent version of the `ztp` plugin.

STEP 3 | Install the Panorama device certificate.

STEP 4 | Register Panorama with the ZTP service.

1. Select **Panorama** > **Zero Touch Provisioning** > **Setup** and edit the **General** ZTP settings.
2. Enter the **Panorama FQDN or IP Address**.
3. (HA only) Enter the **Peer FQDN or IP Address**.
4. Click **OK** to save your configuration changes.

STEP 5 | Create the default device group and template to automatically generate the required configuration to connect your ZTP firewalls to Panorama.

1. **Add Device Group and Template**.
2. Enter the **Device Group** name.
3. Enter the **Template** name.
4. Click **OK** to save your configuration changes.

STEP 6 | Select **Commit** and **Commit to Panorama**.

STEP 7 | Select **Panorama** > **Zero Touch Provisioning** and **Sync to ZTP Service**.

STEP 8 | Configure the ZTP installer administrator account.

1. Select **Panorama** > **Administrators** and **Add** a new admin user.
2. Enter a **Name** and **Password** for the ZTP installer admin.
3. For the **Administrator Type**, select **Custom Panorama Admin**.
4. For the **Profile**, select **installeradmin**.
5. Click **OK** to save your configuration changes.
6. Select **Commit** and **Commit to Panorama**.

STEP 9 | Add ZTP firewalls to Panorama.

1. Log in to the Panorama web interface as the ZTP installer admin.
2. Select **Firewall Registration** and **Add** a new ZTP firewall.
3. Enter the **Serial Number** of the ZTP firewall.
4. Enter the **Claim Key** for the ZTP firewall.
5. Click **OK** to save your configuration changes.
6. Select and **Register** the newly added ZTP firewall.
7. When prompted, click **Yes** to confirm registering the ZTP firewall.

# User-ID Features

- Include Username in HTTP Header Insertion Entries
- Dynamic User Groups

# Include Username in HTTP Header Insertion Entries

You can now dynamically add the user’s domain and username to the HTTP header for the user’s outgoing traffic to allow any secondary appliances that you use with your Palo Alto Networks firewall to receive the user’s information and enforce user-based policy.

*To include the username and domain in the header, the firewall requires the IP address-to-username mapping for the user. If the user is not mapped, the firewall inserts* `unknown` *for both the domain and username in Base64 encoding in the header.*

When you configure a secondary enforcement appliance with your Palo Alto Networks firewall to enforce user-based policy, the secondary appliance may not have the IP address-to-username mapping from the firewall. Transmitting user information to downstream appliances may require deployment of additional appliances such as proxies or negatively impact the user’s experience (for example, users having to log in multiple times). By sharing the user's identity in the HTTP headers, you can enforce user-based policy without negatively impacting the user's experience or deploying additional infrastructure.

When you configure this feature, apply the URL profile to your security policy, and commit your changes, the firewall:

1. Populates the user and domain values with the format of the primary username in the group mapping for the source user.
2. Encodes this information using Base64.
3. Adds the Base64-encoded header to the payload.
4. Routes the traffic to the downstream appliance.

If you want to include the username and domain only when the user accesses specific domains, configure a domain list and the firewall inserts the header only when a domain in the list matches the Host header of the HTTP request.

*The firewall supports header insertion for HTTP/1.x traffic only. HTTP/2 is not supported.*

*This feature supports forward-proxy decryption traffic.*

STEP 1 | Enable User-ID if it is not already enabled.

STEP 2 | Configure group mapping to map users to groups.

STEP 3 | (Optional) To include the username and domain in headers for HTTPS traffic, create a decryption profile to decrypt HTTPS traffic.

STEP 4 | Create or edit a **URL Filtering Profile**.

*The firewall does not insert headers if the action for the URL filtering profile is* **`block`** *for the domain.*

STEP 5 | Define the format for the headers.

You can define up to five headers for each profile.

1. Select **HTTP Header Insertion** and **Add** a new header type.
2. Enter a **Name** (up to 100 characters) for the header.
3. Select **Dynamic Fields** as the header **Type**.
4. **Add** the **Domains** where you want insert headers. When the user accesses a domain in the list, the firewall inserts the specified header.

   Each domain name can be up to 254 characters and you can identify a maximum of 50 domains for each entry. The domain list supports wildcards (for example, **`*.example.com`**); however, as a best practice, nesting wildcards (for example, **`*.*.*`** is not recommended. Do not overlap domains within the same URL profile.
5. **Add** a new **Header** or select **X-Authenticated-User** to edit it.
6. Select a header **Value** format (either **`($domain)\($user)`** or **`WinNT://($domain)/($user)`**) or enter your own format using the **`($domain)`** and **`($user)`** dynamic tokens (for example, **`($user)@($domain)`** for UserPrincipalName).

   > *Do not use the same dynamic token (either **`($user)`** or **`($domain)`**) more than once per value.*

   Each value can be up to 512 characters. The firewall populates the **`($user)`** and **`($domain)`** dynamic tokens using the primary username in the group mapping profile. For example:

   - If the primary username is the sAMAccountName, the value for **`($user)`** is the sAMAccountName and the value for **`($domain)`** is the NetBios domain name.
   - If the primary username is the UserPrincipalName, the **`($user)`** the user account name (prefix) and the **`($domain)`** is the Domain Name System (DNS) name.
7. (Optional) Select **Log** to enable logging for the header insertion.

   Allowed traffic is not logged, so header insertions are not logged for allowed traffic.
8. Select **OK** twice to confirm the HTTP header configuration.

STEP 6 | Apply the URL filtering profile to the security policy rule for HTTP or HTTPS traffic.

1. Select **Policies** > **Security** and select a rule to which to apply the URL filtering profile that you justenabled for header insertion.
2. On the **Actions** tab, select the URL Filtering profile.
3. Click **OK** to save the security policy rule.

STEP 7 | **Commit** your changes.

STEP 8 | To verify the firewall includes the username and domain in the HTTP header:

- Use the **`show user user-ids all`** command to verify the group mapping is correct.
- Use the **`show counter global name ctd_header_insert`** command to view the number of HTTP headers inserted by the firewall.
- If you configured logging in Step 3.7, check the logs for the inserted Base64 encoded payload (for example, **`corpexample\testuser`** would appear in the logs as **`Y29ycGV4YW1wbGVcdGVzdHVzZXI=`**).

# Dynamic User Groups

Dynamic user groups help you to create policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility. Previously, quarantining users in response to suspicious activity meant time- and resource-consuming updates for all members of the group or updating the IP address-to-username mapping to a label to enforce policy at the cost of user visibility, as well as having to wait until the firewall checked the traffic. Now, you can configure a dynamic user group to automatically include users as members without having to manually create and commit policy or group changes and still maintain user-to-data correlation at the device level before the firewall even scans the traffic.

To determine what users to include as members, a dynamic user group uses tags as filtering criteria. As soon as a user matches the filtering criteria, that user becomes a member of the dynamic user group. The tag-based filter uses logical *and* and *or* operators. Each tag is a metadata element or attribute-value pair that you register on the source statically or dynamically. Static tags are part of the firewall configuration, while dynamic tags are part of the runtime configuration. As a result, you don't need to commit updates to dynamic tags if they are already associated with a policy that you have committed on the firewall.

To dynamically register tags, you can use:

- the XML API
- the User-ID agent
- Panorama
- the web interface on the firewall

After you create the group and commit the changes, the firewall registers the users and associated tags then automatically updates the dynamic user group's membership. Because updates to dynamic user group membership are automatic, using dynamic user groups instead of static group objects allows you to respond to changes in user behavior or potential threats without manual policy changes.

The firewall redistributes the tags for the dynamic user group to the listening redistribution agents, which includes other firewalls, Panorama, or a Dedicated Log Collector, as well as Cortex applications.

*To support redistribution for dynamic user group tags, all firewalls must use PAN-OS 9.1 to receive the tags from the registration sources.*

The firewall redistributes the tags for the dynamic user group to the next hop and you can configure log forwarding to send the logs to a specific server. Log forwarding also allows you to use auto-tagging to automatically add or remove members of dynamic user groups based on events in the logs.

Because the dynamic user group itself is static, but the group's membership is dynamic, this allows flexibility with policy creation. For example, if you want the members of the group to return to their original groups after a specific duration of time, configure a timeout for the group. It also allows you to implement information about user behavior from other applications by tagging information from these sources, which updates the dynamic user group membership.

The following example demonstrates how to configure a dynamic user group to deny traffic to users when the firewall detects traffic to questionable sites and use the dynamic user group in a policy to automatically deny traffic to users accessing these sites. The example workflow shows how to configure a dynamic user group that includes users based on their questionable activity and enforce a Security policy for those users that denies access, regardless of the user's device or location, so that when user behavior matches the tags you specify, the firewall adds the user to the dynamic user group and applies the associated policy to deny access.

STEP 1 | Select **Objects** > **Dynamic User Groups** and **Add** a new dynamic user group.

STEP 2 | Define the membership of the dynamic user group.

Create dynamic tags to specify the criteria for members of the dynamic user group. When a user matches the criteria, the firewall adds the user to the group.

1. Enter a **Name** for the group.
2. (Optional) Enter a **Description** for the group.
3. (Panorama only) To share the match criteria of the dynamic user group with all device groups on Panorama, enable **Shared** dynamic user groups.

   When you enable this option, the **Location** column displays whether the match criteria for the dynamic user group is available to every device group on Panorama (**Shared**) or to the selected device group.

   *When you enable this option, Panorama shares the match criteria of the dynamic user group; Panorama does not share the group members.*
4. (Panorama only) To prevent administrators from overriding the settings of this dynamic user group in device groups that inherit the object, enable the **Disable override** option.
5. **Add Match Criteria** using dynamic tags to define the members in the dynamic user group.

   For this example, enter `questionable-activity`.
6. (Optional) Use the **And** or **Or** operators with the tags that you want to use to filter for or match against.
7. Click **OK**.
8. (Optional) Select the **Tags** you want to assign to the group itself.

   *This tag displays in the Tags column in the Dynamic User Group list and defines the dynamic group object, not the members in the group.*
9. Click **OK** and **Commit** your changes.

   *If you update the user group object filter, you must commit the changes to update the configuration.*

STEP 3 | Depending on the log information that you want to use as match criteria, create a log forwarding profile or configure the log settings.

- For Authentication, Data, Threat, Traffic, Tunnel Inspection, URL, and WildFire logs, create a log forwarding profile. This performs the user-to-tag mapping at the device level so that the firewall applies the policy before the firewall detects the traffic.

  1. Select **Objects** > **Log Forwarding** and **Add** a log forwarding profile.
  2. Enter a **Name** for the log forwarding profile then **Add** the **Built-in Actions** you want the firewall to take.
  3. Select **User** as the **Target**.
  4. (Optional) To return dynamic user group members to their original groups after a specific duration of time, enter a **Timeout** value in minutes (default is 0, range is 0-43200).
  5. Specify the **Tags** that define the criteria for the members of the dynamic user group. For this example, enter `questionable-activity`.
- For User-ID, HIP Match, GlobalProtect, and IP-Tag logs, configure the log settings. This performs the user-to-tag mapping at the traffic level so that the firewall applies the policy when it detects the user's traffic.

  1. Select **Device** > **Log Settings**.
  2. Select the type of log that contains the information you want to use for the match criteria and **Add** it.

3. Enter a **Name** and **Add** your **Built-in actions**.
4. Enter a **Name** for each action and select **User** as the **Target** for each action.
5. Select the **Registration** source.
6. (Optional) To return dynamic user group members to their original groups after a specific duration of time, enter a **Timeout** value in minutes (default is 0, range is 0-43200).
7. Specify the **Tags** that define the criteria for the members of the dynamic user group. For this example, enter **`questionable-activity`**.

STEP 4 | Use the dynamic user group in a policy to regulate traffic for the members of the group.

You will need to configure at least two rules: one to allow initial traffic to populate the dynamic user group and one to deny traffic for the activity you want to prevent (in this case, **`questionable-activity`**). To tag users, the rule to allow traffic must have a higher rule number in your rulebase than the rule that denies traffic.

1. Select **Policies** > **Security**.
2. Click **Add** and enter a **Name** and optionally add the **Tags** the policy uses.
3. Add the **Source Zone** to specify the zone where the traffic originates.
4. For the **Source User**, select the dynamic user group from Step 1.
5. Add the **Destination Zone** where the traffic terminates.
6. Select the **Service/URL Category** for the type of traffic you want to prevent.

   For this example, select **questionable** for the rule that denies the traffic.
7. Specify the **Action**.

   For the rule that denies traffic to the dynamic user group members, select **Deny**.
8. **Clone** this rule and **Delete** the **questionable Service/URL Category**, then select **Allow** as the **Action** to create the rule that allows the traffic to populate the dynamic user group members.
9. If you configured a **Log Forwarding** profile in Step 3, select it to add it to the policy.
10. **Commit** your changes.

STEP 5 | (Optional) Refine the group's membership and define the registration source for the user-to-tag mapping updates.

If the initial user-to-tag mapping retrieves users who should not be members or if it does not include users who should be, modify the members of the group to include the users for whom you want to enforce the policy and specify the source for the mappings.

1. In the **Users** column, select **more**.
2. **Register Users** to add them to the group and select the **Registration Source** for the tags and user-to-tag mappings.
   - **Local** (Default)—Register the tags and mappings for the dynamic user group members locally on the firewall.
   - **Panorama User-ID Agent**—Register the tags and mappings for the dynamic user group members on a User-ID agent connected to Panorama. If the dynamic user group originates from Panorama, the row displays in yellow and the group name, description, match criteria, and tags are read-only. However, you can still register or unregister users from the group.
   - **Remote device User-ID Agent**—Register the tags and mappings for the dynamic user group members on a remote User-ID agent. To select this option, you must first configure an HTTP server profile.
3. Select the **Tags** you want to register on the source using the tags you used to configure the group.
4. (Optional) To return dynamic user group members to their original groups after a specific duration of time, enter a **Timeout** value in minutes (default is 0, range is 0-43200).
5. **Add** or **Delete** users as necessary.
6. (Optional) **Unregister Users** to remove their tags and user-to-tag mappings.

STEP 6 | Verify the firewall correctly populates the users in the dynamic user group.

1. Confirm the **Dynamic User Group** column in the Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, and Tunnel Inspection logs displays the dynamic user groups correctly.
2. Use the **`show user group list dynamic`** command to display a list of all dynamic user groups as well as the total number of dynamic user groups.
3. Use the **`show object registered-user all`** command to display a list of users who are registered members of dynamic user groups.
4. Use the **`show user group name`** ***`group-name`*** command to display information about the dynamic user group, such as the source type.

STEP 7 | Monitor the users in your dynamic user groups to track user activity.

1. In the Application Command Center (ACC), create a global or local filter to track the dynamic user group (**Add** > **User** > **Dynamic User Group**).
2. Generate user activity reports for members of dynamic user groups (**Monitor** > **PDF Reports** > **User Activity Report**) to determine if more malicious activity occurs.

# GlobalProtect Features

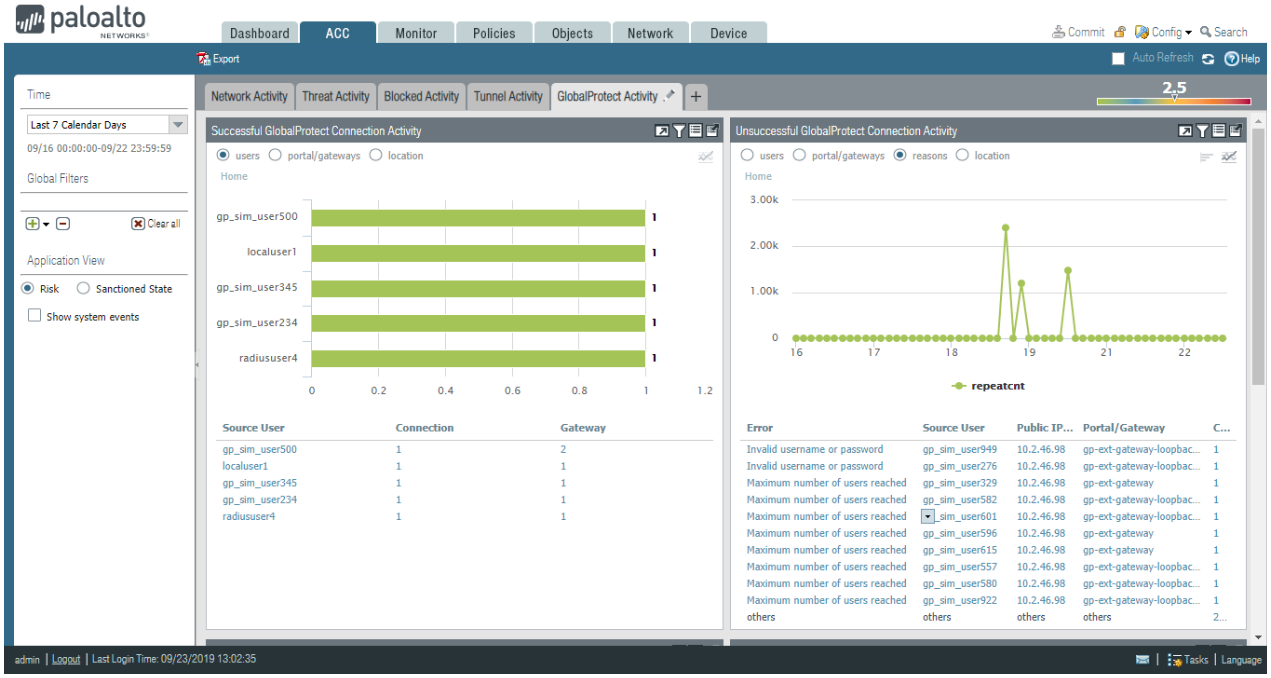
# Enhanced Logging for GlobalProtect

To help you monitor and troubleshoot issues with your GlobalProtect deployment, PAN-OS now provides the following logging enhancements for GlobalProtect:

- GlobalProtect Activity Charts and Graphs on the ACC
- New GlobalProtect Log Category
- New GlobalProtect Admin Role
- Log Forwarding for GlobalProtect Logs
- Custom Reports for GlobalProtect

These features are available for any Palo Alto Networks next-generation firewall deployed as a GlobalProtect gateway or portal.

## GlobalProtect Activity Charts and Graphs on the ACC



| Source User | Connection | Gateway |
|---|---|---|
| gp_sim_user500 | 1 | 2 |
| localuser1 | 1 | 1 |
| gp_sim_user345 | 1 | 1 |
| gp_sim_user234 | 1 | 1 |
| radiususer4 | 1 | 1 |

| Error | Source User | Public IP... | Portal/Gateway | C... |
|---|---|---|---|---|
| Invalid username or password | gp_sim_user949 | 10.2.46.98 | gp-ext-gateway-loopbac... | 1 |
| Invalid username or password | gp_sim_user276 | 10.2.46.98 | gp-ext-gateway-loopbac... | 1 |
| Maximum number of users reached | gp_sim_user329 | 10.2.46.98 | gp-ext-gateway | 1 |
| Maximum number of users reached | gp_sim_user582 | 10.2.46.98 | gp-ext-gateway-loopbac... | 1 |
| Maximum number of users reached | ▾_sim_user601 | 10.2.46.98 | gp-ext-gateway-loopbac... | 1 |
| Maximum number of users reached | gp_sim_user596 | 10.2.46.98 | gp-ext-gateway | 1 |
| Maximum number of users reached | gp_sim_user615 | 10.2.46.98 | gp-ext-gateway | 1 |
| Maximum number of users reached | gp_sim_user557 | 10.2.46.98 | gp-ext-gateway-loopbac... | 1 |
| Maximum number of users reached | gp_sim_user580 | 10.2.46.98 | gp-ext-gateway-loopbac... | 1 |
| Maximum number of users reached | gp_sim_user922 | 10.2.46.98 | gp-ext-gateway-loopbac... | 1 |
| others | others | others | others | 2... |

The ACC displays a graphical view of user activity in your GlobalProtect deployment on the GlobalProtect Activity tab. The following charts are available:

- **Successful GlobalProtect Connection Activity**—Chart view of GlobalProtect connection activity over the selected time period. Use the toggle at the top of the chart to switch between connection statistics by users, portals and gateways, and location.
- **Unsuccessful GlobalProtect Connection Activity**—Chart view of unsuccessful GlobalProtect connection activity over the selected time period. Use the toggle at the top of the chart to switch between connection statistics by users, portals and gateways, and location. To help you identify and troubleshoot connection issues, you can also view the reasons chart or graph. For this chart, the ACC indicates the error, source user, public IP address and other information to help you identify and resolve the issue quickly.

- **GlobalProtect Deployment Activity**—Chart view summary of your deployment. Use the toggle at the top of the chart to view the distribution of users by authentication method, GlobalProtect app version, and operating system version.

The GlobalProtect Activity charts and graphs are also interactive and support similar drill-down functionality to other ACC charts and graphs.

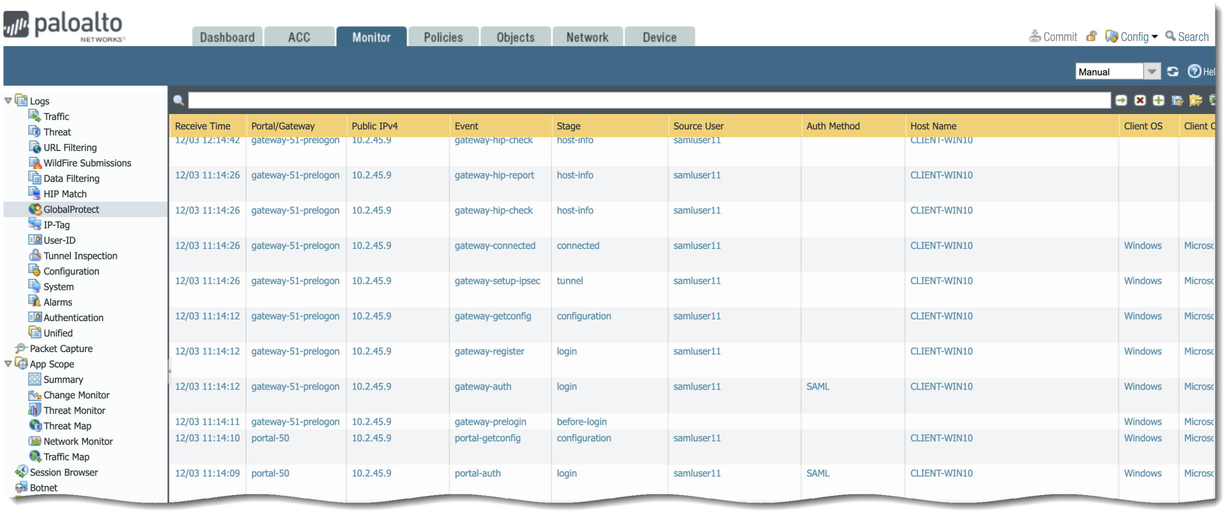
In addition, the **GlobalProtect Host Information** widget under the Network Activity tab is now renamed **HIP Information**.

# New GlobalProtect Log Category

PAN-OS now moves GlobalProtect logs to a new dedicated page within **Monitor** > **Logs**. This page enables you to view the following GlobalProtect events in one place:

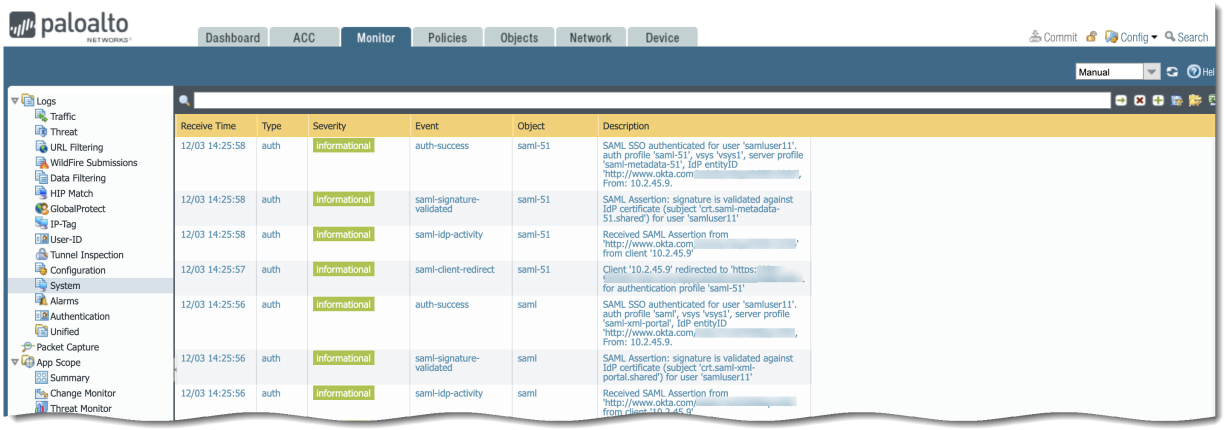
- System logs related to GlobalProtect.

  GlobalProtect authentication event logs remain in **Monitor** > **Logs** > **System**; however, the new GlobalProtect logs display information that shows the authentication method that is used. The following screenshot shows an example of logs in the new **Monitor** > **Logs** > **GlobalProtect** page; note the **Auth Method** of **SAML**.



| Receive Time | Portal/Gateway | Public IPv4 | Event | Stage | Source User | Auth Method | Host Name | Client OS | Client C |
|---|---|---|---|---|---|---|---|---|---|
| 12/03 12:14:42 | gateway-51-prelogon | 10.2.45.9 | gateway-hip-check | host-info | samluser11 | | CLIENT-WIN10 | | |
| 12/03 11:14:26 | gateway-51-prelogon | 10.2.45.9 | gateway-hip-report | host-info | samluser11 | | CLIENT-WIN10 | | |
| 12/03 11:14:26 | gateway-51-prelogon | 10.2.45.9 | gateway-hip-check | host-info | samluser11 | | CLIENT-WIN10 | | |
| 12/03 11:14:26 | gateway-51-prelogon | 10.2.45.9 | gateway-connected | connected | samluser11 | | CLIENT-WIN10 | Windows | Micros |
| 12/03 11:14:26 | gateway-51-prelogon | 10.2.45.9 | gateway-setup-ipsec | tunnel | samluser11 | | CLIENT-WIN10 | Windows | Micros |
| 12/03 11:14:12 | gateway-51-prelogon | 10.2.45.9 | gateway-getconfig | configuration | samluser11 | | CLIENT-WIN10 | Windows | Micros |
| 12/03 11:14:12 | gateway-51-prelogon | 10.2.45.9 | gateway-register | login | samluser11 | | CLIENT-WIN10 | Windows | Micros |
| 12/03 11:14:12 | gateway-51-prelogon | 10.2.45.9 | gateway-auth | login | samluser11 | SAML | CLIENT-WIN10 | Windows | Micros |
| 12/03 11:14:11 | gateway-51-prelogon | 10.2.45.9 | gateway-prelogin | before-login | | | | Windows | Micros |
| 12/03 11:14:10 | portal-50 | 10.2.45.9 | portal-getconfig | configuration | samluser11 | | CLIENT-WIN10 | Windows | Micros |
| 12/03 11:14:09 | portal-50 | 10.2.45.9 | portal-auth | login | samluser11 | SAML | CLIENT-WIN10 | Windows | Micros |

  Compare these to the authentication-related logs that are in **Monitor** > **Logs** > **System**.



| Receive Time | Type | Severity | Event | Object | Description |
|---|---|---|---|---|---|
| 12/03 14:25:58 | auth | informational | auth-success | saml-51 | SAML SSO authenticated for user 'samluser11'. auth profile 'saml-51', vsys 'vsys1', server profile 'saml-metadata-51', IdP entityID 'http://www.okta.com[redacted], From: 10.2.45.9. |
| 12/03 14:25:58 | auth | informational | saml-signature-validated | saml-51 | SAML Assertion: signature is validated against IdP certificate (subject 'crt.saml-metadata-51.shared') for user 'samluser11' |
| 12/03 14:25:58 | auth | informational | saml-idp-activity | saml-51 | Received SAML Assertion from 'http://www.okta.com,[redacted]' from client '10.2.45.9' |
| 12/03 14:25:57 | auth | informational | saml-client-redirect | saml-51 | Client '10.2.45.9' redirected to 'https:[redacted]. for authentication profile 'saml-51' |
| 12/03 14:25:56 | auth | informational | auth-success | saml | SAML SSO authenticated for user 'samluser11'. auth profile 'saml', vsys 'vsys1', server profile 'saml-xml-portal', IdP entityID 'http://www.okta.com/[redacted], From: 10.2.45.9. |
| 12/03 14:25:56 | auth | informational | saml-signature-validated | saml | SAML Assertion: signature is validated against IdP certificate (subject 'crt.saml-xml-portal.shared') for user 'samluser11' |
| 12/03 14:25:56 | auth | informational | saml-idp-activity | saml | Received SAML Assertion from 'http://www.okta.com/[redacted] from client '10.2.45.9' |

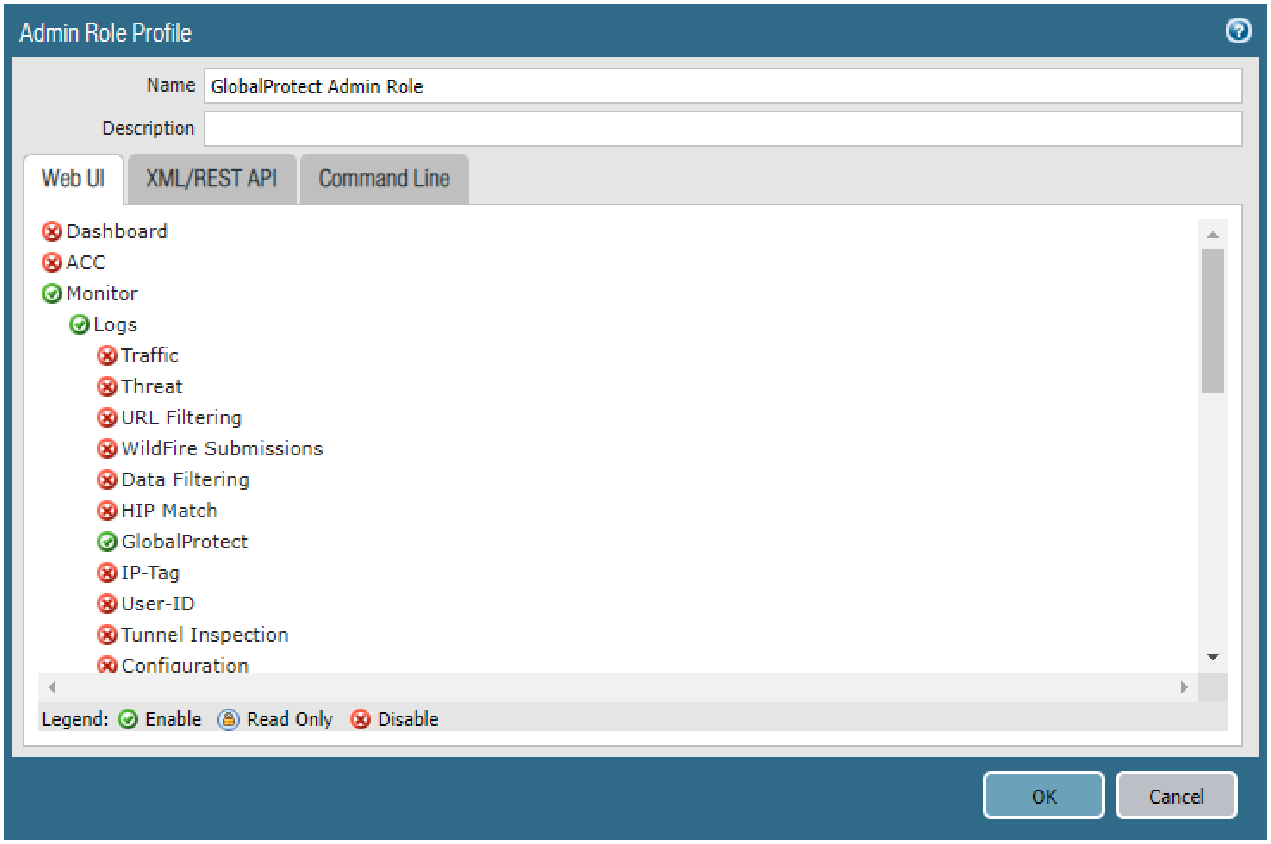
- LSVPN/satellite events.

- GlobalProtect portal and gateway logs.
- Clientless VPN logs.

The new log category eliminates the need for using complex log queries to locate GlobalProtect logs. You can also sort, filter, and query the GlobalProtect logs.

## New GlobalProtect Admin Role

If access to GlobalProtect logs and data is a concern (such as for regulatory compliance or data privacy concerns), you can restrict access to these logs by creating an Admin Role profile and specifying the **GlobalProtect** role to enable, disable, or provide read-only access to the GlobalProtect logs.



Admin Role Profile

Name: GlobalProtect Admin Role

Description:

✗ Dashboard
✗ ACC
✓ Monitor
  ✓ Logs
    ✗ Traffic
    ✗ Threat
    ✗ URL Filtering
    ✗ WildFire Submissions
    ✗ Data Filtering
    ✗ HIP Match
    ✓ GlobalProtect
    ✗ IP-Tag
    ✗ User-ID
    ✗ Tunnel Inspection
    ✗ Configuration

Legend: ✓ Enable 🔒 Read Only ✗ Disable

## Log Forwarding for GlobalProtect Logs

You can now forward GlobalProtect logs to an external service such as a syslog receiver or ticketing system. In cases where some teams in your organization can achieve greater efficiency by monitoring only the GlobalProtect logs that are relevant to their operations, you can create forwarding filters based on GlobalProtect log attributes. For example, you can filter by:

- GlobalProtect authentication events generated by GlobalProtect (type eq globalprotect)

  GlobalProtect authentication events generated by the authentication service (type eq auth) remain in **Monitor** > **Logs** > **System**.
- All other GlobalProtect events (non-authentication)

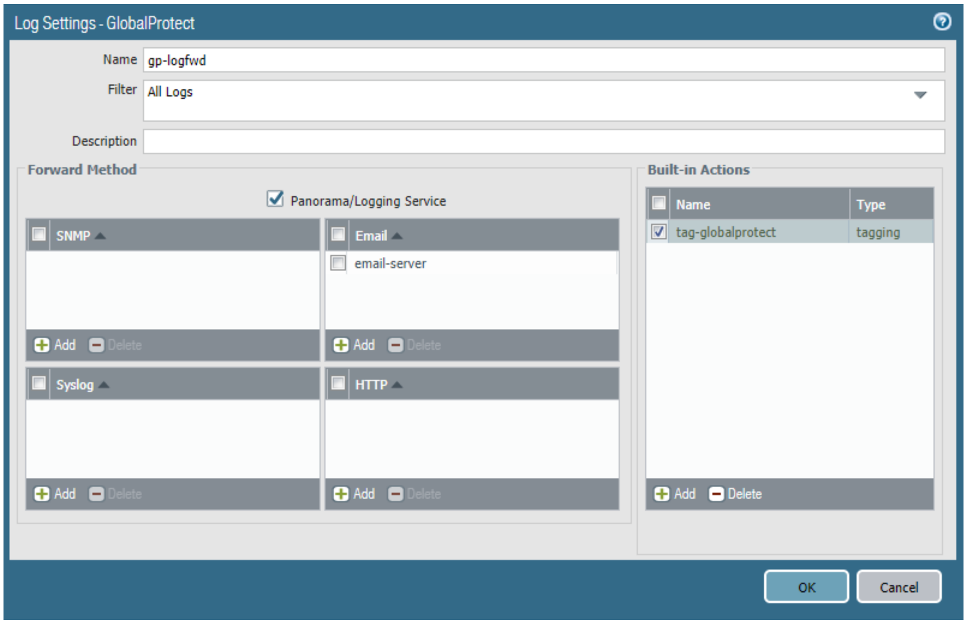
Palo Alto Networks firewalls forward GlobalProtect logs using the following format. To facilitate parsing, the delimiter is a comma: each field is a comma-separated value (CSV) string.

**Format:** domain, receive_time, serial, seqno, actionflags, type, subtype, config_ver, time_generated, vsys, eventid, stage, auth_method, tunnel_type, srcuser, srcregion, machinename, public_ip, public_ipv6, private_ip, private_ipv6, hostid, serialnumber, client_ver, client_os, client_os_ver, repeatcnt, reason, error, opaque, status, location, login_duration, connect_method, error_code, portal

To configure log forwarding for GlobalProtect logs:

STEP 1 | Configure a server profile for each external service that will receive log information.

STEP 2 | Configure the destinations for GlobalProtect logs.



Log Settings - GlobalProtect

Name: gp-logfwd

Filter: All Logs

Description:

Forward Method

☑ Panorama/Logging Service

| □ | Email |
|---|---|
| □ | email-server |

Built-in Actions

| □ | Name | Type |
|---|---|---|
| ☑ | tag-globalprotect | tagging |

You can also add or remove tags from a source or destination IP address in a log entry.

STEP 3 | Commit and verify your changes.

## Custom Reports for GlobalProtect

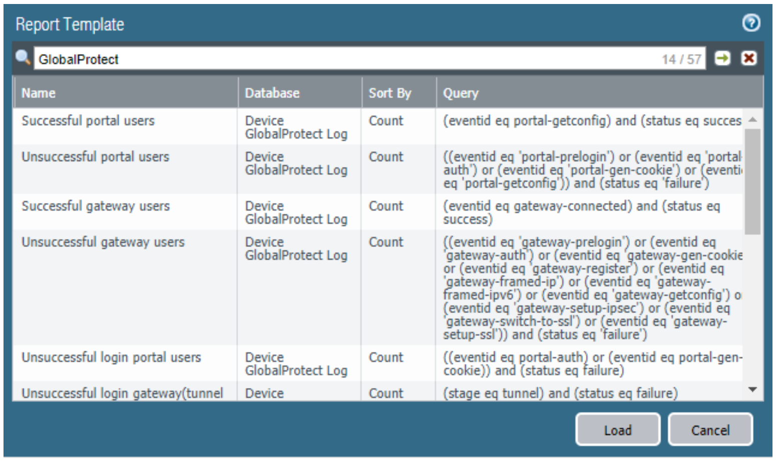
You can configure custom reports based on GlobalProtect logs that the firewall generates immediately (on demand) or on schedule (each night).

To Generate a Custom Report for GlobalProtect:

STEP 1 | Select **Monitor** > **Manage Custom Reports**.

STEP 2 | Click **Add** and then enter a **Name** for the report.

STEP 3 | To base a report on an predefined template, click **Load Template** and choose the template. You can then edit the template and save it as a custom report.



Report Template

GlobalProtect 14 / 57

| Name | Database | Sort By | Query |
|---|---|---|---|
| Successful portal users | Device GlobalProtect Log | Count | (eventid eq portal-getconfig) and (status eq succes |
| Unsuccessful portal users | Device GlobalProtect Log | Count | ((eventid eq 'portal-prelogin') or (eventid eq 'portal-auth') or (eventid eq 'portal-gen-cookie') or (eventi eq 'portal-getconfig')) and (status eq 'failure') |
| Successful gateway users | Device GlobalProtect Log | Count | (eventid eq gateway-connected) and (status eq success) |
| Unsuccessful gateway users | Device GlobalProtect Log | Count | ((eventid eq 'gateway-prelogin') or (eventid eq 'gateway-auth') or (eventid eq 'gateway-gen-cookie or (eventid eq 'gateway-register') or (eventid eq 'gateway-framed-ip') or (eventid eq 'gateway-framed-ipv6') or (eventid eq 'gateway-getconfig') o (eventid eq 'gateway-setup-ipsec') or (eventid eq 'gateway-switch-to-ssl') or (eventid eq 'gateway-setup-ssl')) and (status eq 'failure') |
| Unsuccessful login portal users | Device GlobalProtect Log | Count | ((eventid eq portal-auth) or (eventid eq portal-gen-cookie)) and (status eq failure) |
| Unsuccessful login gateway(tunnel | Device | Count | (stage eq tunnel) and (status eq failure) |

STEP 4 | If you choose to build the report from scratch, select the database you want to use for the report as **Device GlobalProtect Log**.

STEP 5 | Select the **Scheduled** check box to run the report each night. The report is then available for viewing in the **Reports** column on the side.

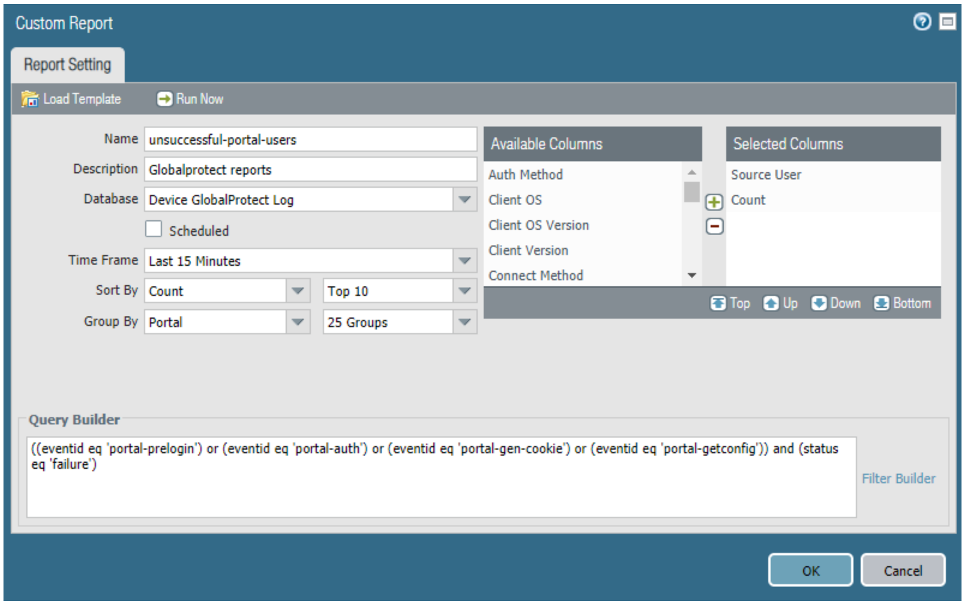
STEP 6 | Define the filtering criteria. Select the **Time Frame**, the **Sort By** order, **Group By** preference, and select the columns that must display in the report.

STEP 7 | (Optional) Select the **Query Builder** attributes if you want to further refine the selection criteria. To build a report query, specify the following and click **Add**. Repeat as needed to construct the full query.

- **Connector**—Choose the connector (and/or) to precede the expression you are adding.
- **Negate**—Select the check box to interpret the query as a negation. If, for example, you choose to match entries in the last 24 hours and/or are originating from the untrust zone, the negate option causes a match on entries that are not in the past 24 hours and/or are not from the untrust zone.
- **Attribute**—Choose a data element. The available options depend on the choice of database.
- **Operator**—Choose the criterion to determine whether the attribute applies (such as =). The available options depend on the choice of database.
- **Value**—Specify the attribute value to match.

For example, to build a report for GlobalProtect portal users with unsuccessful login attempts, use a query similar to the following:

```
((eventid eq 'portal-prelogin') or (eventid eq 'portal-auth') or (eventid
eq 'portal-gen-cookie') or (eventid eq 'portal-getconfig')) and (status eq
'failure')
```



Custom Report

Report Setting

Name: unsuccessful-portal-users

Description: Globalprotect reports

Database: Device GlobalProtect Log

□ Scheduled

Time Frame: Last 15 Minutes

Sort By: Count | Top 10

Group By: Portal | 25 Groups

Available Columns: Auth Method, Client OS, Client OS Version, Client Version, Connect Method

Selected Columns: Source User, Count

Query Builder

```
((eventid eq 'portal-prelogin') or (eventid eq 'portal-auth') or (eventid eq 'portal-gen-cookie') or (eventid eq 'portal-getconfig')) and (status
eq 'failure')
```

STEP 8 | To test the report settings, select **Run Now**. Modify the settings as required to change the information that is displayed in the report.

STEP 9 | Click **OK** to save the custom report.

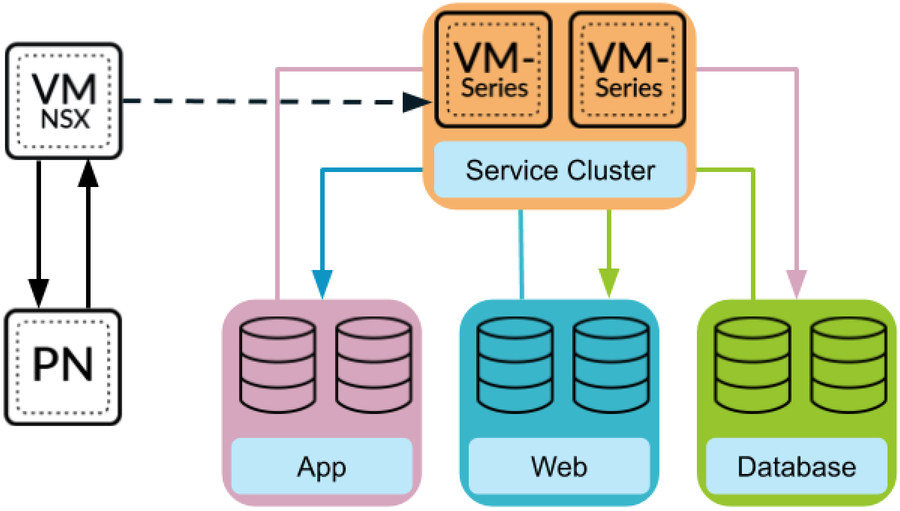
# Virtualization Features

# VM-Series Firewall on VMware NSX-T (East-West)

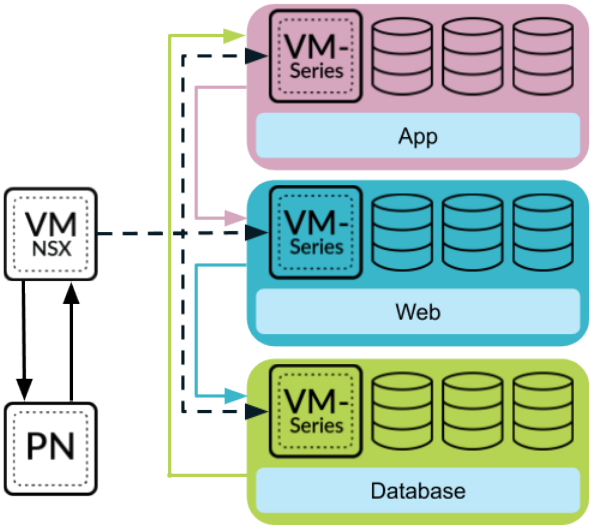
You can now deploy the VM-Series firewall on VMware NSX-T as a partner service to provide comprehensive visibility and safe application enablement of all East-West traffic in your NSX-T software-defined data center. The VM-Series firewall as a partner service enables micro-segmentation that allows you to protect your data center, enable granular access control inter-tier application traffic.

The VM-Series firewall on VMware NSX-T (East-West) requires the Panorama plugin for VMware NSX 3.1.0 or later.

- **Service Cluster**—Multiple instances of the VM-Series firewall are deployed on a single ESXi cluster. NSX-T manager redirects traffic between VMs and security groups to the VM-Series firewall before it continues to the intended destination.



- **Host-Based**—The VM-Series firewall is deployed on each ESXi hosts in your software-defined data center. Traffic between guests on the same host is inspected by the local firewall, so it does not need to leave the host for inspection. Traffic leaving the host is inspected by the firewall before reaching the vSwitch.



Deploying the VM-Series firewall to secure East-West traffic in your NSX-T software-defined data center requires the following steps.

1. **Register the VM-Series firewall as a service**—Use Panorama to connect to your VMware NSX-T manager. After establishing communication with NSX-T Manager, configure the service definition.

   Additionally, NSX-T Manager uses this connection to send updates on the changes in the NSX-T environment with Panorama.
2. **Deploy the VM-Series firewall per host or in a service cluster**—NSX-T Manager uses the information pushed from Panorama in the service definition to deploy the VM-Series firewall. Choose a where the VM-Series firewall will be deployed (in a service cluster or on each ESXi host) and how NSX-T provides a management IP address to the VM-Series firewall.
3. **The VM-Series connects to Panorama and sends security policy to the VM-Series firewall**—The VM-Series firewall then connects to Panorama to obtain its license. Panorama gets the license from the Palo Alto Networks update server and sends it to the firewall. When the firewall gets its license, it reboots and comes back up with a serial number. When the firewall reconnects to Panorama after rebooting, it is added to device group and template stack defined in the service definition and Panorama pushes the appropriate security policy to that firewall. The firewall is now ready to secure traffic in your NSX-T data center.

   NSX-T Manager sends real-time updates about changes in the virtual environment to Panorama. As Panorama receives updates from NSX-T Manager, it sends those updates from its managed VM-Series firewalls as changes in dynamic address groups. This allows firewalls to apply the correct security policy to traffic flowing to and from virtual machines in your NSX-T data center.
4. **Create network introspection rules to redirect traffic to the VM-Series firewall**—On the NSX-T Manager, create a service chain and network introspection rules that redirect traffic in your NSX-T data center.