PAN-OS® 8.1 New Features Guide
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade to PAN-OS 8.1</td>
<td>5</td>
</tr>
<tr>
<td>Upgrade/Downgrade Considerations</td>
<td>7</td>
</tr>
<tr>
<td>Upgrade the Firewall to PAN-OS 8.1</td>
<td>12</td>
</tr>
<tr>
<td>Determine the Upgrade Path to PAN-OS 8.1</td>
<td>12</td>
</tr>
<tr>
<td>Upgrade Firewalls Using Panorama</td>
<td>13</td>
</tr>
<tr>
<td>Upgrade a Standalone Firewall to PAN-OS 8.1</td>
<td>18</td>
</tr>
<tr>
<td>Upgrade an HA Firewall Pair to PAN-OS 8.1</td>
<td>20</td>
</tr>
<tr>
<td>Downgrade from PAN-OS 8.1</td>
<td>25</td>
</tr>
<tr>
<td>Downgrade a Firewall to a Previous Feature Release</td>
<td>25</td>
</tr>
<tr>
<td>Downgrade a Firewall to a Previous Maintenance Release</td>
<td>26</td>
</tr>
<tr>
<td>Downgrade a Windows Agent from PAN-OS 8.1</td>
<td>26</td>
</tr>
<tr>
<td>App-ID Features</td>
<td>29</td>
</tr>
<tr>
<td>SaaS Application Hosting Characteristics</td>
<td>31</td>
</tr>
<tr>
<td>Simplified App-ID</td>
<td>34</td>
</tr>
<tr>
<td>New App-ID Threshold</td>
<td>34</td>
</tr>
<tr>
<td>New App-ID Characteristic</td>
<td>35</td>
</tr>
<tr>
<td>Extended Policy Impact Review for Content Releases</td>
<td>37</td>
</tr>
<tr>
<td>Coverage Change Details for Modified App-IDs</td>
<td>38</td>
</tr>
<tr>
<td>HTTP Header Insertion and Modification</td>
<td>39</td>
</tr>
<tr>
<td>Service-Based Session Timeouts</td>
<td>40</td>
</tr>
<tr>
<td>Virtualization Features</td>
<td>41</td>
</tr>
<tr>
<td>VM-50 Lite</td>
<td>43</td>
</tr>
<tr>
<td>Integration with Azure Security Center</td>
<td>44</td>
</tr>
<tr>
<td>Support for Azure Application Insights</td>
<td>46</td>
</tr>
<tr>
<td>Bootstrapping Enhancements for VM-Series on Azure</td>
<td>48</td>
</tr>
<tr>
<td>VM-Series Firewall on Google Cloud Platform</td>
<td>51</td>
</tr>
<tr>
<td>Deploy the VM-Series Firewall from Google Cloud Platform Marketplace</td>
<td>51</td>
</tr>
<tr>
<td>Enable Google Stackdriver Monitoring</td>
<td>52</td>
</tr>
<tr>
<td>Enable VM-Series Firewall to Track Changes on Google Cloud Platform VMs</td>
<td>53</td>
</tr>
<tr>
<td>Decryption Features</td>
<td>55</td>
</tr>
<tr>
<td>Decryption Broker</td>
<td>57</td>
</tr>
<tr>
<td>Automatic SAN Support for SSL Decryption</td>
<td>58</td>
</tr>
<tr>
<td>HSM Client Upgrade and SafeNet HSM Cluster Support</td>
<td>59</td>
</tr>
<tr>
<td>ECDSA Certificate Support for SSL Decryption with HSMs</td>
<td>60</td>
</tr>
<tr>
<td>Decryption Port Mirroring Support Extension</td>
<td>61</td>
</tr>
<tr>
<td>Panorama Features</td>
<td>63</td>
</tr>
<tr>
<td>Device Monitoring on Panorama</td>
<td>65</td>
</tr>
<tr>
<td>Configuration Reusability for Templates and Template Stacks</td>
<td>67</td>
</tr>
<tr>
<td>Panorama Virtual Appliance and Virtual Dedicated Log Collector on AWS</td>
<td>69</td>
</tr>
<tr>
<td>Panorama Virtual Appliance and Virtual Dedicated Log Collector on AWS GovCloud</td>
<td>71</td>
</tr>
<tr>
<td>Panorama Virtual Appliance and Virtual Dedicated Log Collector on Azure</td>
<td>73</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Panorama Virtual Appliance and Virtual Dedicated Log Collector on Google Cloud</td>
<td>74</td>
</tr>
<tr>
<td>Panorama Virtual Appliance and Virtual Dedicated Log Collector on KVM</td>
<td>76</td>
</tr>
<tr>
<td>Panorama Virtual Appliance and Virtual Dedicated Log Collector on Hyper-V</td>
<td>78</td>
</tr>
<tr>
<td>Virtual Dedicated Log Collector on ESXi</td>
<td>80</td>
</tr>
<tr>
<td>Streamlined Panorama Deployment for Application and Threat Content Updates</td>
<td>81</td>
</tr>
<tr>
<td>Content Update Revert from Panorama</td>
<td>83</td>
</tr>
<tr>
<td>Direct Query of PA-7000 Series Firewalls from Panorama</td>
<td>84</td>
</tr>
<tr>
<td>Panorama Interconnect</td>
<td>85</td>
</tr>
<tr>
<td>Content Inspection Features</td>
<td>87</td>
</tr>
<tr>
<td>SCTP Security</td>
<td>89</td>
</tr>
<tr>
<td>Rapid Deployment of the Latest Threat Prevention</td>
<td>91</td>
</tr>
<tr>
<td>Tools to Avoid or Mitigate Content Update Issues</td>
<td>92</td>
</tr>
<tr>
<td>Authentication Features</td>
<td>95</td>
</tr>
<tr>
<td>Extensible Authentication Protocol (EAP) Support for RADIUS</td>
<td>97</td>
</tr>
<tr>
<td>Authentication Using Custom Certificates for WildFire, PAN-DB, and Between Log Collectors</td>
<td>100</td>
</tr>
<tr>
<td>GlobalProtect Features</td>
<td>103</td>
</tr>
<tr>
<td>Optimized Split Tunneling for GlobalProtect</td>
<td>105</td>
</tr>
<tr>
<td>Kerberos Authentication Support for macOS</td>
<td>110</td>
</tr>
<tr>
<td>SAML SSO for GlobalProtect on Chromebooks</td>
<td>115</td>
</tr>
<tr>
<td>OPSWAT SDK V4 Support</td>
<td>117</td>
</tr>
<tr>
<td>Management Features</td>
<td>119</td>
</tr>
<tr>
<td>Rule Usage Tracking</td>
<td>121</td>
</tr>
<tr>
<td>Configuration Table Export</td>
<td>123</td>
</tr>
<tr>
<td>Reporting Engine Enhancements</td>
<td>124</td>
</tr>
<tr>
<td>Enhanced Application Logging</td>
<td>126</td>
</tr>
<tr>
<td>Networking Features</td>
<td>127</td>
</tr>
<tr>
<td>Tunnel Content Inspection Logging</td>
<td>129</td>
</tr>
<tr>
<td>Dynamic IP Address Support for Destination NAT</td>
<td>130</td>
</tr>
<tr>
<td>FQDN Support for IKE Gateway Peer IP Address</td>
<td>132</td>
</tr>
<tr>
<td>Configuration Capacity Improvements</td>
<td>133</td>
</tr>
<tr>
<td>Refresh of Default Trusted CAs</td>
<td>135</td>
</tr>
<tr>
<td>ARP Cache Timeout</td>
<td>136</td>
</tr>
<tr>
<td>User-ID Features</td>
<td>137</td>
</tr>
<tr>
<td>Support for Multiple Username Formats</td>
<td>139</td>
</tr>
<tr>
<td>WildFire Features</td>
<td>143</td>
</tr>
<tr>
<td>WildFire Appliance-to-Appliance Encryption</td>
<td>145</td>
</tr>
</tbody>
</table>
Upgrade to PAN-OS 8.1

> Upgrade/Downgrade Considerations
> Upgrade the Firewall to PAN-OS 8.1
> Downgrade from PAN-OS 8.1
Upgrade/Downgrade Considerations

The following table lists the new features that have upgrade or downgrade impacts. Make sure you understand all potential changes before you upgrade to or downgrade from a PAN-OS 8.1 release. For additional information about PAN-OS 8.1 releases, refer to the PAN-OS 8.1 Release Notes.

For M-100 appliances running in Panorama mode, Palo Alto Networks recommends upgrading the memory to 32GB to avoid the risk of running out of memory for management and log collection tasks. See M-100 Memory Upgrade Guide for more information.

Table 1: PAN-OS 8.1 Upgrade/Downgrade Considerations

<table>
<thead>
<tr>
<th>Feature</th>
<th>Upgrade Considerations</th>
<th>Downgrade Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Third-Party SFP Transceivers</td>
<td>A small percentage of writable third-party SFP transceivers (not purchased from Palo Alto Networks) can stop working or experience other issues after you upgrade the firewall to which they are connected to a PAN-OS 8.0 or PAN-OS 8.1 release. Because it is typically impossible to know if a third-party SFP is writable, Palo Alto Networks® recommends that, if your firewall uses third-party SFPs, you do not upgrade to a PAN-OS 8.0 or PAN-OS 8.1 release until you are able to upgrade to a maintenance release for each that addresses this issue. Additionally, when you are ready to upgrade, make sure that you do not reboot the firewall after you download and install the PAN-OS 8.1 (or PAN-OS 8.0) base image until after you download and install a maintenance release that contains the fix for this issue. This is true when upgrading to PAN-OS 8.1 even if you addressed this issue when you upgraded to a PAN-OS 8.0 maintenance release that includes this fix. For more information about this known issue and maintenance releases related to this issue, refer to the PAN-OS 8.0 or PAN-OS 8.1 release notes, as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Support for Multiple Username Formats</td>
<td>During an upgrade, the User Name in the User Objects section for the Group Mapping profile will be</td>
<td>During a downgrade, the Primary Username is used to retrieve the user name and the Allow matching</td>
</tr>
<tr>
<td>Feature</td>
<td>Upgrade Considerations</td>
<td>Downgrade Considerations</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td><strong>Extensible Authentication Protocol (EAP) Support for RADIUS</strong></td>
<td>Auto has been removed from list of available authentication protocols for a RADIUS Server Profile. During the upgrade, all existing RADIUS Server Profiles using PAP or CHAP will continue to use the selected authentication protocol. If the RADIUS server profile used Auto, the firewall will attempt to change to CHAP or PAP, based on which protocol was in use before the upgrade. If the firewall cannot determine which one was used, CHAP is selected. After you upgrade, Panorama templates use CHAP as the default authentication protocol. If your Panorama templates used the Auto authentication protocol and your RADIUS server requires PAP, update your Panorama template to use PAP to avoid having to log out and log in again after the upgrade.</td>
<td>Any RADIUS Server Profiles configured to use EAP (PEAP-MSCHAPv2, PEAP with GTC, or EAP-TTLS with PAP) will be migrated to Auto (where CHAP is attempted first, then PAP). Any additional options associated with the EAP protocol, such as Outer Identity and Certificate Profiles, will be removed from the configuration.</td>
</tr>
<tr>
<td><strong>HSM Client Upgrade and SafeNet HSM Cluster Support</strong></td>
<td>PAN-OS 8.1 upgrades Thales nShield client version 11.62 to version 12.30. You can upgrade the firewall to use SafeNet client version 5.4.2 or 6.2.2. These HSM client versions provide necessary compatibility with HSM server versions. With an upgraded HSM client version on PAN-OS, you must ensure the corresponding HSM server version is also upgraded.</td>
<td>A PAN-OS release is tied to an HSM client version, so if you downgrade from PAN-OS 8.1 to a release prior to PAN-OS 8.0.2 (for example, PAN-OS 8.0.0 or 8.0.1), the downgrade will fail. Downgrading from PAN-OS 8.1 to 8.0.2 or a later release will succeed and the HSM client version will be retained.</td>
</tr>
<tr>
<td>Feature</td>
<td>Upgrade Considerations</td>
<td>Downgrade Considerations</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FQDN Support for IKE Gateway Peer IP Address</td>
<td>Downgrading will remove the address objects, address groups, and FQDNs from an IKE VPN Peer IP address, so unless the peer IP address is a static IP address, the downgrade will fail.</td>
<td></td>
</tr>
<tr>
<td>Dynamic IP Address Support for Destination NAT</td>
<td>Downgrading means that a translated destination NAT address specifying <strong>Dynamic IP (with session distribution)</strong> isn't supported, so the downgrade will fail.</td>
<td></td>
</tr>
<tr>
<td>FQDN Refresh Time</td>
<td>If you downgrade a VM-Series firewall that used an FQDN Refresh Time in the range 60-599 seconds, the downgrade will fail because the downgraded release doesn't support an FQDN refresh time that fast; it supports a range of 600-14,399 seconds. Select <strong>Device &gt; Setup &gt; Services</strong>, change the 8.1 FQDN Refresh Time to a value in the range 600-14,399 seconds, commit, and then downgrade.</td>
<td></td>
</tr>
<tr>
<td>DNS Suffix Support</td>
<td>In PAN-OS 8.0.x and earlier releases, you can only add up to 10 DNS suffixes to the GlobalProtect gateway configuration (<strong>Network &gt; GlobalProtect &gt; Gateways &gt; &lt;gateway-config&gt; &gt; GlobalProtect Gateway Configuration &gt; Agent &gt; Network Services &gt; DNS Suffix</strong>). You must remove additional DNS suffixes from the configuration prior to downgrading from PAN-OS 8.1.0 to PAN-OS 8.0.x or earlier releases. In Panorama 8.1.0 and earlier releases, you can only push up to 10 DNS suffixes to firewalls running PAN-OS 8.0.x and earlier releases.</td>
<td></td>
</tr>
</tbody>
</table>
### Upgrade Considerations

**OPSWAT SDK V4 Support**

PAN-OS 8.1 supports OPSWAT SDK V4. When you upgrade to PAN-OS 8.1, the **Antivirus** and **Anti-Spyware** HIP categories merge to form the new **Anti-Malware** category. Vendor and product names are also updated for OPSWAT SDK V4 in all HIP categories.

The latest GlobalProtect data file must be installed on your firewall following an upgrade to PAN-OS 8.1. Until the data file is installed, HIP functionality is not available. For PAN-OS 8.1, the GlobalProtect data file is for OPSWAT SDK V4. GlobalProtect data file installation can only be triggered when a data file update schedule is configured under **Device > Dynamic Updates > GlobalProtect Data File**. We recommend that you set the **Schedule** recurrence to **Hourly**.

When configurations are pushed from Panorama 8.1 to a PAN-OS 8.0 or earlier firewall, the **Anti-Malware** category is dropped from the HIP Match log and HIP Object. You must manually reconfigure the **Antivirus** and **Anti-Spyware** categories to display this information in the OPSWAT SDK V3 format. Vendor and product names may also be different for OPSWAT SDK V3, so you must review and manually reconfigure as necessary.

When downgrading a firewall from PAN-OS 8.1 to an earlier PAN-OS release, Panorama will display the content version installed on the firewall while it was running PAN-OS 8.1 regardless of the version currently running on the firewall.

### Downgrade Considerations

PAN-OS 8.0 and earlier releases do not support OPSWAT SDK V4. When you downgrade to an earlier version of PAN-OS, the **Anti-Malware** category is dropped. You must manually reconfigure the **Antivirus** and **Anti-Spyware** categories to display this information in the OPSWAT SDK V3 format. After your system is rebooted, all HIP match logs are persistent, while all existing HIP reports are deleted.

The latest GlobalProtect data file must be installed on your firewall following a downgrade to PAN-OS 8.0 or earlier releases. Until the data file is installed, HIP functionality is not available. For PAN-OS 8.0 and earlier releases, the GlobalProtect data file is for OPSWAT SDK V3. GlobalProtect data file installation can only be triggered when a data file update schedule is configured under **Device > Dynamic Updates > GlobalProtect Data File**. We recommend that you set the **Schedule** recurrence to **Hourly**.

When downgrading a firewall from PAN-OS 8.1 to an earlier PAN-OS release, Panorama will display the content version installed on the firewall while it was running PAN-OS 8.1 regardless of the version currently running on the firewall.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Upgrade Considerations</th>
<th>Downgrade Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual appliance is in Legacy mode on upgrade, the mode will be preserved. However, if you change the Panorama virtual appliance mode, you cannot change back into Legacy mode.</td>
<td>Management Only Mode</td>
<td>When downgrading a Panorama appliance from PAN-OS 8.1 to an earlier PAN-OS release, the Panorama appliance must be in Panorama mode or Log Collector mode. Downgrade from PAN-OS 8.1 is not supported for a Panorama appliance in Management Only mode.</td>
</tr>
<tr>
<td>Management Only Mode</td>
<td>On upgrade to PAN-OS 8.1, templates with devices attached to them will be converted into template stacks that contain the original template and have the device attached to the template stack. The template stack name will be <code>&lt;Template Name&gt;_mig_stack</code>.</td>
<td>Configuration Reusability for Templates and Template Stacks</td>
</tr>
<tr>
<td>VM-Series Firewall for VMware NSX</td>
<td>You must install VMware NSX plugin 2.0.1 before upgrading Panorama to 8.1. You must select a template stack when configuring a service definition for your VM-Series for NSX deployment. Selecting a template causes a commit failure when attempting to commit the changes to Panorama.</td>
<td></td>
</tr>
</tbody>
</table>
Upgrade the Firewall to PAN-OS 8.1

How you upgrade to PAN-OS 8.1 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 8.1 Release Notes and then follow the procedure specific to your deployment:

- Determine the Upgrade Path to PAN-OS 8.1
- Upgrade Firewalls Using Panorama
- Upgrade a Standalone Firewall to PAN-OS 8.1
- Upgrade an HA Firewall Pair to PAN-OS 8.1

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

Determine the Upgrade Path to PAN-OS 8.1

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.

<table>
<thead>
<tr>
<th>Installed PAN-OS Version</th>
<th>Recommended Upgrade Path to PAN-OS 8.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0.x</td>
<td>If you are already running a PAN-OS 8.0 release, download and install the latest PAN-OS 8.0 maintenance release and reboot. You can then proceed to Upgrade the Firewall to PAN-OS 8.1.</td>
</tr>
</tbody>
</table>
| 7.1.x                    | □ Download and install the latest PAN-OS 7.1 maintenance release and reboot.  
                          □ Download and install PAN-OS-8.0.0 and, as a best practice, reboot.  
                          □ Download and install the latest PAN-OS 8.0 maintenance release and reboot.  
                          Proceed to Upgrade the Firewall to PAN-OS 8.1. |
| 7.0.x                    | □ Download and install the latest PAN-OS 7.0 maintenance release and reboot.  
                          □ Download and install PAN-OS 7.1.0.  
                          □ Download and install the latest PAN-OS 7.1 maintenance release and reboot.  
                          □ Download and install PAN-OS 8.0.0 and, as a best practice, reboot.  
                          □ Download and install the latest PAN-OS 8.0 maintenance release and reboot.  
                          Proceed to Upgrade the Firewall to PAN-OS 8.1. |
| 6.1.x                    | □ Download and install the latest 6.1 maintenance release and reboot.  
                          □ Download and install PAN-OS 7.0.1 (7.0.1 is the base image for the 7.0 release, not 7.0.0).  
                          □ Download and install the latest PAN-OS 7.0 maintenance release and reboot.  
                          □ Download and install PAN-OS 7.1.0.  
                          □ Download and install the latest PAN-OS 7.1 maintenance release and reboot.  
                          □ Download and install PAN-OS 8.0.0 and, as a best practice, reboot.  
                          □ Download and install the latest PAN-OS 8.0 maintenance release and reboot.  
                          Proceed to Upgrade the Firewall to PAN-OS 8.1. |

**Upgrade Firewalls Using Panorama**

Review the PAN-OS 8.1 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 updates server, follow the procedure for deploying updates to firewalls when Panorama is not internet-connected so that you can manually download images to Panorama and then distribute the images to firewalls.

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 8.1 before upgrading the managed firewalls to this version.
- Ensure that firewalls are connected to a reliable power source. A loss of power during an upgrade can make a firewall unusable.

**STEP 1** | 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.

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 2** | 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 8.1. Make sure to follow the Best Practices for Application and Threat Content 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.

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.
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 `set max-num-images count <number>` CLI command to increase the maximum.

**STEP 3 | (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**.

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

**STEP 4 | Determine the Upgrade Path to PAN-OS 8.1**

You cannot skip installation of any feature release versions in the path from the currently running PAN-OS version to PAN-OS 8.1.0. 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 5 | Download the target PAN-OS 8.1 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.
For example, to upgrade your PA-220, PA-3050, and PA-5250 firewalls to PAN-OS 8.1.0, download the PanOS_220-8.1.0, PanOS_3000-8.1.0, and PanOS_5200-8.1.0 images. After you successfully download an image, the Action column changes to Install for that image.

STEP 6 | Install the PAN-OS 8.1 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-220 firewalls, click Install in the row that corresponds to PanOS_220-8.1.0.

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.

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 8.1.0 for the firewalls you upgraded. Also verify that the HA status of any passive firewalls you upgraded is still passive.

**STEP 7 | (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.


   4. Go back to the High Availability widget on the Dashboard and verify that Local changed to Passive and Peer changed to 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 8 |** 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.
STEP 9 | (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 8.1

Review the PAN-OS 8.1 Release Notes and then use the following procedure to upgrade a firewall that is not in an HA configuration to PAN-OS 8.1.

If your firewalls are configured to forward samples to a WF-500 appliance for analysis, you must upgrade the WildFire appliance to PAN-OS 8.1 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.

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

3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.
STEP 2 | 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 8.1 release. Make sure to follow the Best Practices for Application and Threat Content Updates.

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

2. If the firewall is not running the minimum required content release version or a later version required for PAN-OS 8.1, 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 8.1

You cannot skip installation of any feature release versions in the path from the currently running PAN-OS version to PAN-OS 8.1.0.

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 8.1.

If your firewall does not have internet access from the management port, you can download the software image from the Palo Alto Networks Support Portal and then manually Upload it to your firewall.
1. Select Device > Software and click Check Now to display the latest PAN-OS updates.
2. Locate and Download PAN-OS 8.1.0.
3. After you download the image (or, for a manual upgrade, after you upload the image), Install the image.

<table>
<thead>
<tr>
<th>Version</th>
<th>Size</th>
<th>Release Date</th>
<th>Available</th>
<th>Currently Installed</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.0</td>
<td>465 MB</td>
<td>2018/02/23 20:35:29</td>
<td>Uploaded</td>
<td></td>
<td>Install</td>
</tr>
<tr>
<td>8.0.6</td>
<td>348 MB</td>
<td>2017/12/13 22:31:09</td>
<td>Uploaded</td>
<td></td>
<td>Reinstall</td>
</tr>
<tr>
<td>8.0.6.1</td>
<td>348 MB</td>
<td>2017/12/12 23:12:43</td>
<td>Uploaded</td>
<td></td>
<td>Release Notes</td>
</tr>
<tr>
<td>8.0.4</td>
<td>295 MB</td>
<td>2017/07/26 14:25:57</td>
<td></td>
<td>Download</td>
<td>Release Notes</td>
</tr>
<tr>
<td>8.0.3</td>
<td>298 MB</td>
<td>2017/06/14 14:30:38</td>
<td></td>
<td>Download</td>
<td>Release Notes</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Start Time</th>
<th>From Zone</th>
<th>To Zone</th>
<th>Source</th>
<th>Destination</th>
<th>Start Port</th>
<th>To Port</th>
<th>Protocol</th>
<th>Application</th>
<th>Rule</th>
<th>Ingress LIF</th>
<th>Egress LIF</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/02 12:04:27</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Required Infrastructure</td>
<td>ethernet</td>
<td>123216</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09/03 15:08:29</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>1128002</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09/04 15:27:01</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>145</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09/07 10:35:22</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>144421</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09/05 13:54:11</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>148</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09/09 18:09:58</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>11761</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09/12 13:12:53</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>145</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/09 11:27:10</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>31084967</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/09 14:45:06</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>5042962</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/09 22:58:27</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>4949041</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/13 15:20:19</td>
<td>T-Zone</td>
<td>T-Zone</td>
<td>web-browsing</td>
<td>Allowed Personal Apps</td>
<td>ethernet</td>
<td>109</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Upgrade an HA Firewall Pair to PAN-OS 8.1

Review the PAN-OS 8.1 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**.

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

3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

**STEP 2 |** 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 8.1 release. Make sure to follow the **Best Practices for Application and Threat Content Updates**.

1. Select **Device > Dynamic Updates** and check which **Applications** or **Applications and Threats** to determine which update is Currently Installed.
2. If the firewalls are not running the minimum required content release version or a later version required for PAN-OS 8.1, 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.

3. Commit the change.

### STEP 5 | Determine the Upgrade Path to PAN-OS 8.1

You cannot skip installation of any feature release versions in the path from the currently running PAN-OS version to PAN-OS 8.1.0.

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 8.1 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.
Because the User-ID mappings are managed differently in 8.1.0, after the passive peer is upgraded and available, the mappings are not synced until both peers are running the same release version.

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 8.1.0.

If your firewall does not have internet access from the management port, you can download the software image from the PaloAltoNetworksSupport 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.

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.

STEP 7 | If you have enabled User-ID, the firewall connects to the User-ID sources to repopulate the mappings. To confirm the firewall has successfully repopulated the mappings, use the following CLI commands:

- show user ip-user-mapping all
- show user group list

After the firewall repopulates the mappings, it can enforce user-based policy and user-based visibility is available.

STEP 8 | Install PAN-OS 8.1 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 8.1.0.
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
   ```

**STEP 9 |** Verify that the other peer has successfully received the mappings using the CLI commands from Step 7.

**STEP 10 |** 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 11 |** 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 8.1

The way you downgrade a firewall from PAN-OS 8.1 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 8.0.2 to 7.1.7 or from 7.1.6 to 7.0.9) or downgrading to a maintenance release version within the same feature release (where the third digit in the release version changes, for example, from 8.0.2 to 8.0.0). When you downgrade from one feature release to an earlier feature release, you can migrate the configuration from the later release to accommodate new features. To migrate the PAN-OS 8.1 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 8.1

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 8.1.0 to 8.0.7), not to downgrades to maintenance releases within the same feature release version (for example, 8.0.7 to 8.0.4).

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 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.

- Export named configuration snapshot (Device > Setup > Operations).
- Select the XML file that contains your running configuration (for example, running-config.xml) and click OK to export the configuration file.
- 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 8.1 and are downgrading to PAN-OS 8.0.7, select autosave-8.0.7.
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 Firewall to a Previous Maintenance Release**

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

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

**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 Windows Agent from PAN-OS 8.1**

After you uninstall the PAN-OS 8.1 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.
App-ID Features

- SaaS Application Hosting Characteristics
- Simplified App-ID
- HTTP Header Insertion and Modification
- Service-Based Session Timeouts
SaaS Application Hosting Characteristics

You can now identify, assess, and reduce risks related to SaaS applications with unfavorable hosting characteristics by leveraging the enhanced ACC filters in App-ID™. To help you determine which applications you should allow in your environment, five new application hosting characteristics are now available: data breaches, poor terms of service, no certifications, poor financial viability, and IP-based access restrictions. You can use these application characteristics to gain visibility, control and the information you need to make informed decisions about the apps on your network, and define actions to eliminate risks or prevent future violations.

The enhanced ACC filters allow you to view the detailed risk profiles and usage statistics for the SaaS applications on your network based on the following hosting characteristics:

<table>
<thead>
<tr>
<th>SaaS Application Characteristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Breaches</td>
<td>It is important for you to know if the SaaS application has ever had an intentional or unintentional release of secure information to an untrusted environment without proper information security precautions. Data loss and exfiltration is a possible risk when you use SaaS applications that do not disclose breaches or that have been breached within the past three years.</td>
</tr>
<tr>
<td>Poor Terms of Service</td>
<td>Applications with poor terms of service such as termination of service at any time for any reason, or making your sensitive data public for non-payment can make your enterprise vulnerable to loss of intellectual property, data, or nonavailability of service.</td>
</tr>
<tr>
<td>No Certifications</td>
<td>Certifications can help you assess applications to verify if the application has gone through certain basic security precautions that have been validated and officially recorded by a certification party. Most certifications are not a one-time evaluation and provide you the assurance that the security of the application is periodically evaluated. Applications are checked for compliance with industry certifications such as SOC1, SOC2, SSAE16, PCI, HIPAA, FINRAA, or FEDRAMP.</td>
</tr>
<tr>
<td>Poor Financial Viability</td>
<td>If the application vendor goes out of business, the liquidation activities can have a serious impact your enterprise. For example, during liquidation the customer data is considered an asset and sold, potentially exposing your IP and losing the data to the liquidator. This characteristic checks for applications with the potential to be out of business within the next 18 to 24 months and reports the applications with poor financial viability.</td>
</tr>
<tr>
<td>IP-based Restrictions</td>
<td>An application without IP-based restrictions lack the ability to restrict end-user access from outside of the corporate network, and can expose your enterprise data to end-users outside of your known enterprise IP range (such as a corporate campus).</td>
</tr>
<tr>
<td>SaaS Application Characteristic</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>The data for the IP-based Restrictions characteristic is available to view in the Network Activity graphs and for generating a custom report.</td>
</tr>
</tbody>
</table>

For ease of use, the applications with unfavorable hosting characteristics are displayed automatically in the predefined Application Usage Report.

*The application usage report displays in a new window, so your browser must allow pop-ups.*

*If the preview window does not open, refer to your browser documentation for the steps to enable pop-ups.*

*The Applications with Risky Characteristics displays on page 2 of the report.*
Applications with Risky Characteristics

**Data Breaches**
Applications that may have released secure information to an untrusted source within the past three years.

- **g     gotomypc-file-transfer** 1 Users 503.2M
- **g     gotomypc-printing** 1 Users 7.8M

**Poor Terms of Service**
Applications with unfavorable terms of service that can compromise an enterprise.

- **s     sendspace** 1 Users 9.7M
- **v     via3** 1 Users 7.2M

**No Certifications**
Applications lacking current compliance to industry programs or certifications such as SOC2, SSAE16, PCI, HIPAA, FINRA, or FEDRAMP.

- **g     gotomypc-file-transfer** 1 Users 503.2M
- **4     4shared** 1 Users 9.3M

**Poor Financial Viability**
Applications with the potential to be out of business within the next 18 to 24 months.

- **s     screencast-base** 1 Users 5.9M

For a more tailored view, you can also use the characteristics to build a custom report.
Simplified App-ID

App-ID identifies the applications traversing your network—regardless of port, protocol, encryption, or any evasive tactics—so that you can safely enable desired applications and block unwanted applications. Palo Alto Networks releases new App-IDs on a monthly basis that your security policy can begin to enforce without any additional configuration. While this enables the firewall to dynamically control application traffic with ever-increasing precision, changes in how the firewall enforces applications can potentially impact availability for the mission-critical applications on which your organization relies.

Now, you no longer need to weigh availability for mission-critical applications against equipping the firewall with the latest application knowledge; with the following options, you can do both, and it’ll be easier for you to move to and maintain an application-based security policy:

- **New App-ID Threshold** on page 34—Fine tune content update installation thresholds so that threat updates install immediately as they’re released, and new App-IDs are installed only after you’ve had an opportunity to make any necessary security policy updates.
- **New App-ID Characteristic** on page 35—Automatically allow new App-IDs in critical categories (like software-development), and get visibility into new App-ID activity on your network.
- **Extended Policy Impact Review for Content Releases**—Now you can see how currently installed content releases impact security policy enforcement, and policy review is extended to include modified App-IDs. (Previously, you could only perform a policy impact review for new App-IDs before you installed a content release).
- **Coverage Change Details for Modified App-IDs**—Get details on how coverage for modified applications is now expanded or more precise.

New App-ID Threshold

New and updated application and threat signatures are released together in a single package as Applications and Threats content updates. Previously, this meant that you had to install threat updates and new and modified applications at the same time, and choose one of two approaches to deploying content updates:

- A mission-critical approach, where you delay content update installation until you can assess it’s impact to application availability.
- A security-first approach, where you install application and threat updates as they’re made available; you prioritize the latest threat protection over a possible impact to application availability.

Now, the New App-ID Threshold allows you to install content updates that include new App-IDs on a separate schedule from those that don’t. Especially if your business has a mission-critical approach, this gives you extra time to review how new App-IDs impact security policy enforcement, and make any necessary policy updates.

To configure a New App-ID Threshold, modify the **Applications and Threats Update Schedule** (select **Device > Dynamic Updates > Schedule**).
The New App-ID Threshold must always be a value greater than the overall content update threshold. The example above shows what an Application and Threats Update Schedule might look like if you decide on a mission-critical approach to deploying content updates. Note that the overall content Threshold is set to 12 hours, while the new App-ID threshold is set to 48 hours.

**New App-ID Characteristic**

The New App-ID characteristic is now found throughout the firewall web interface; in several different contexts, it enables you to filter for only the App-IDs that were introduced in the most recently installed content releases. This means that you can enforce brand new App-IDs without adjusting your security policy, and monitor new App-ID activity.

- **Ensure Critical New App-IDs are Allowed**—Use the New App-ID characteristic in policy to allow critical applications based on category (for example, always allow authentication or software development apps). Ensure availability for these critical applications, while continuing to get the latest App-ID updates.
- **Get Increased Visibility Into New App-ID Activity**—Monitor and generate reports for new App-IDs. What you learn can help you make the right decisions about how you to update your security policy to enforce the most recently-categorized App-IDs.

Regardless of where you use it, the New App-ID characteristic always matches to only the new App-IDs in the most recently installed content releases. When a new content release is installed, the new App-ID characteristic automatically begins to enforce only the new App-IDs in that content release version.

**Ensure Critical New App-IDs are Allowed**

New App-IDs can cause a change in policy enforcement for traffic that is newly-identified as belonging to a certain application. You can now add the predefined New App-ID application filter to a security policy rule in order to use only new App-IDs as match criteria for the rule. You can choose to enforce all new App-IDs, or target the security policy rule to enforce certain types of new App-IDs (for example, enforce only authentication or software development apps). Set the security policy rule to Allow to ensure that even if an App-ID release introduces expanded or more precise coverage for critical applications, the firewall continues to allow them. New App-IDs are released on the third Tuesday of every month, and the application filter provides coverage for only those applications in the latest release. This gives you a month’s time (or, if the firewall is not installing content updates on a schedule, until the next time you manually install content) to assess how newly-categorized applications might impact security policy enforcement and make any necessary adjustments.

**STEP 1 | Select Objects > Application Filters and Add a new application filter.**
STEP 2 | Define the types of new applications for which you want to ensure constant availability based on subcategory or characteristic. For example, select the category “auth-service” to ensure that any newly-installed applications that are known to perform or support authentication are allowed.

STEP 3 | Only after narrowing the types of new applications that you want to allow immediately upon installation, select Apply to New App-IDs only.

STEP 4 | Select Policies > Security and add or edit a security policy rule that is configured to allow matching traffic.

STEP 5 | Select Application and add the new Application Filter to the policy rule as match criteria.

STEP 6 | Click OK and Commit to save your changes.

STEP 7 | To continue to adjust your security policy to account for any changes to enforcement that new App-IDs introduce:

- Extended Policy Impact Review for Content Releases—See how the newly-installed App-IDs impact your existing security policy rules.

Get Increased Visibility Into New App-ID Activity

The New App-ID characteristic enables you to monitor new applications on your network, so that you can better assess the security policy updates you might want to make. Use the New App-ID characteristic on the ACC to get visibility into the new applications on your network, and to generate reports that detail newly-categorized application activity.

- Generate a report with details specifically regarding new applications (applications introduced only in the latest content release).
• Use the ACC to monitor new application activity: select ACC and under Global Filters, select Application > Application Characteristics > New App-ID.

Extended Policy Impact Review for Content Releases

Policy impact review is now available for installed content releases and includes details on how modified App-IDs affect security policy enforcement. Previously, policy impact review details, where you can view all security policy rules where application enforcement might have changed due to a content update, were only available for downloaded content updates and detailed only how new App-IDs affected security policy rules.

Take the following steps to see a list of the applications modified in a content release and assess how those changes impact security policy enforcement. Importantly, updates to applications with network-wide impact (for example, LDAP or IKE) are prominently flagged as a Policy Review Recommendation.

**STEP 1** | Select Device > Dynamic Updates and Download the latest Applications and Threats content release.

**STEP 2** | For any content release (downloaded or currently installed) select either Review Policies or Review Apps in the Action column of the content update row.
STEP 3 | **Review Apps** to see a list of all applications that are modified in a content release, and see details for each application. In addition to modified applications being listed, updates to applications with network-wide impact (for example, LDAP or IKE) are prominently flagged as a **Policy Review Recommendation**. This signals to you to evaluate potential changes in enforcement for those critical applications.

STEP 4 | **Review Policies** to see the security policy rules that might enforce traffic differently now that the application is modified.

**Coverage Change Details for Modified App-IDs**

Application details now include information on: **Expanded Coverage**, **Remove False Positive**, and application metadata changes. The **Expanded Coverage** and **Remove False Positive** fields both indicate how the application's coverage has changed (it's either more comprehensive or has been narrowed) and a clock icon indicates a metadata change, where certain application details are updated.
HTTP Header Insertion and Modification

Unsanctioned usage of SaaS applications can be a way for your users to transmit sensitive information outside of your network, usually by accessing a consumer version of an application. However, if you need to allow access to the enterprise version of these applications for specific individuals or organizations, then you can't block the SaaS application entirely. With the HTTP header insertion and modification feature, you can now manage HTTP header information to disallow SaaS consumer accounts while allowing a specific enterprise account.

Because many SaaS applications allow or disallow access to applications based on information contained in specific HTTP headers, you can use predefined header insertion rules to manage access to popular SaaS applications. Predefined rules are specific to particular SaaS applications. Currently there are four available predefined applications: Google, Dropbox, YouTube, and Office 365. These applications (and any additional applications that might be predefined in the future) are populated and maintained by Palo Alto Networks® using content updates. If a SaaS vendor changes its implementation so that additional header or domain information is needed, Palo Alto Networks will use a content update to modify the relevant predefined rule for you.

If you want to perform HTTP header insertion for an application that is not yet predefined in a content update, you can create a custom rule. Custom rules allow you to manage custom HTTP headers but you can also use them to manage standard HTTP headers depending on your requirements.

Custom rules that you create will never be managed or modified by Palo Alto Networks. It is your responsibility to maintain the custom rules that you create so that they accurately interact with the SaaS application.

You don't need a URL Filtering license to use this feature.
Service-Based Session Timeouts

You can now more easily maintain custom timeouts for applications as you move from a port-based policy to an application-based policy. Previously, you might have had to override App-ID (losing application visibility) or create a custom App-ID (expending time and research) in order to maintain custom timeouts for applications.

To get started, configure custom timeout settings as part of a service object:

![Service Configuration Interface](image)

Then add the service object in a policy rule to apply the custom timeouts to the application(s) the rule enforces. See the full workflow to Maintain Custom Timeouts for Legacy Applications—you can follow these same steps to apply custom timeouts to user groups.
Virtualization Features

- VM-50 Lite
- Integration with Azure Security Center
- Support for Azure Application Insights
- Bootstrapping Enhancements for VM-Series on Azure
- VM-Series Firewall on Google Cloud Platform
VM-50 Lite

The VM-50 Lite provides an alternative for environments where hardware resources are constrained; specifically environments where the standard VM-50’s 4.5 GB memory footprint is too large. The VM-50 Lite requires 4GB of memory instead of the 4.5GB required by the standard VM-50.

The VM-50 Lite is a mode of operation, not a new model. Enabling lite mode uses the same license as the standard VM-50 but changes to a VM-50 Lite when you lower the allocated memory. And while the VM-50 Lite has lower capacity, it has the same performance of the standard VM-50.

The VM-50 Lite does not support the Application Command Center (ACC).
Integration with Azure Security Center

The **VM-Series firewall integration with Azure Security Center** provides a single pane of glass for high-priority security alerts so you can start triaging an incident directly from the Azure Security Center dashboard. To start using this integration, you must enable Azure Security Center on your Azure subscription.

When you deploy a VM-Series firewall on Azure directly from Azure Security Center, the firewall is automatically configured with two example Security policy rules to safely inspect and allow inbound web-browsing traffic and outbound traffic, and it includes a log forwarding rule to send security-related logs to Azure. With this log forwarding profile, Threat and WildFire Submissions logs of low, medium, high, or critical severity generated on the firewall are displayed as security alerts on the Azure Security Center dashboard.

Currently Azure restricts you from deploying a multi NIC appliance in an existing resource group. Therefore, you cannot deploy the VM-Series firewall in a resource group where you have deployed the workloads you want to secure. To work around this limitation and make practical use of the default configuration for the VM-Series firewall, you can stage a security risk and deploy a workload with a public IP address that is exposed to the internet. Doing so will trigger the Azure Security Center recommendation for a next-generation firewall, and you can use this recommendation to deploy the firewall in an empty resource group. The deployment workflow is the same as the Azure Marketplace for VM-Series firewall. After you deploy the VM-Series firewall, delete the internet exposed workload, you can deploy your applications or workloads in the resource group when needed within the resource group where you’ve already deployed the firewall.
Azure Security Center can also automatically discover an existing or new VM-Series firewall instance that you launch with PAN-OS 8.1 from the Azure marketplace or have a custom deployment using the Azure CLI, PowerShell or ARM template. To enable the discovery of the VM-Series firewall as a Security Solution on the Azure Security Center dashboard, you must have the Standard tier of Azure Security Center enabled on your subscription. The workflow to forward security-related logs from the VM-Series firewall to Azure Security Center is more involved and requires you to use an intermediate Linux virtual machine and configure Syslog forwarding to send the required logs from the VM-Series firewall. If you have already configured your firewall, you can manually attach the Azure Security Center- default Log Forwarding profile directly on the firewall or use Panorama templates and device groups to enable managed firewalls to forward logs to Azure Security Center.
Support for Azure Application Insights

In PAN-OS 8.1, the VM-Series firewall on Azure includes support for natively publishing PAN-OS metrics to an Azure Application Insights instance where you can monitor firewall performance and health status, view trends on performance and usage patterns, and set up alerts to detect anomalies proactively.

**STEP 1** | Set up an Application Insights instance of type **General**. Refer to Azure documentation for details on how to create an Application Insights resource.

**STEP 2** | Log in to the VM-Series firewall on Azure and configure it to publish PAN-OS metrics to Azure Application Insights.

**STEP 3** | Select **Device** > **Setup** > **Operations**.

**STEP 4** | Select **Enable Application Insights**, and copy and paste the **Instrumentation Key** from the Azure portal. The firewall requires this key to authenticate to the Application Insights instance and publish metrics to it.

**STEP 5** | **Commit** the changes.

**STEP 6** | Verify that the firewall is publishing metrics.

Log in to the Azure portal and on the Application Insights instance that you entered above, view the custom metrics on the Metrics Explorer.
Bootstrapping Enhancements for VM-Series on Azure

The solution template in the Azure Marketplace has been updated to enable bootstrapping, and you can now use Azure file storage to upload the configuration files and licenses to easily bootstrap the VM-Series firewall at launch. In order to bootstrap successfully, you must provide the name of the storage account that holds the bootstrap folders and the keys to authenticate for access the storage account.

**STEP 1 |** Log in to the Azure portal (https://portal.azure.com).

**STEP 2 |** Set up the storage account with a File service. The File service allows the VM-Series firewalls to read files stored there and get provisioning information at launch.

If you are using the solution template in the Azure marketplace to deploy the VM-Series, make sure to keep this storage account in a different resource group that the one in which you plan to deploy the firewall. This is because the solution template can be deployed in either a new or empty resource group.

Within the File service, you must create a File share. In the File share you must Add the directory structure for the bootstrap package so that you can upload the files required for bootstrapping. Optionally, you can specify a Share-directory. If you have a common File share that serves as a repository for bootstrap configuration for different set ups, using a share-directory gives you the flexibility to create a folder hierarchy and access a specific set of sub-folders within the common File share.
STEP 3 | Add the information to bootstrap the firewall, when you Deploy the VM-Series firewall.

1. Select Enable Bootstrap yes.
2. Enter the Storage Account Name that holds the bootstrap package.
3. Enter the Storage Account Access Key. This firewall needs this access key to authenticate to the storage account and access the files stored in it.
4. Add the File share name to which you have uploaded the files required for bootstrapping the firewall. The storage account must be set up with the correct folder structure for the bootstrapping.

STEP 4 | Verify that you have successfully bootstrapped the VM-Series firewall.

1. Select Dashboard > Resource Groups, select the resource group.
2. Select Settings > Deployments > Deployment History for detailed status.
STEP 5 | To publish PAN-OS metrics to Azure Application Insights, see Support for Azure Application Insights.
VM-Series Firewall on Google Cloud Platform

You can now deploy the VM-Series firewall on a Google Compute Engine instance within a Google Cloud Platform project to secure your applications and workloads.

The VM-Series firewall on Google Cloud Platform can publish custom PAN-OS metrics to Google Stackdriver. With Stackdriver Monitoring, you can monitor the firewall, and set up alerts based on firewall health and performance.

You can also enable any firewall that runs PAN-OS 8.1 (virtual or physical) to monitor application workloads deployed on Google Compute Engine instances. With an awareness of virtual machine adds, moves, or deletes within a Google VPC, you can create security policy rules that automatically adapt to changes in your application environment.

- Deploy the VM-Series Firewall from Google Cloud Platform Marketplace
- Enable Google Stackdriver Monitoring
- Enable VM-Series Firewall to Track Changes on Google Cloud Platform VMs

Deploy the VM-Series Firewall from Google Cloud Platform Marketplace

The VM-series firewall is part of your Google project, using the VPC networks to communicate with other compute engine instances. In addition to serving as an internet gateway, the VM-series firewall can secure east-west traffic between VPCs to ensure data protection compliance and application access.
Google Marketplace provides templates based on license types. The templates deploy an instance of the VM-Series firewall with a management interface and two dataplane interfaces.

Before you deploy the VM-Series firewall, you must choose a project in your organization, and create a minimum of three networks and subnetworks that the firewall requires at launch.

**STEP 1** | Locate the VM-Series firewall listing in Google Marketplace.

1. Log in to the Google Cloud Console.
2. From the Products and Services menu, choose **Marketplace**.
3. Search for “VM-Series”.
4. Select one of the VM-Series licensing options.

**STEP 2** | Click **Launch on Compute Engine**.

**STEP 3** | Deploy the VM-Series Firewall from Google Cloud Platform Marketplace.

**Enable Google Stackdriver Monitoring**

You can enable any firewall that runs PAN-OS 8.1 (virtual or physical) to monitor application workloads deployed on Google Compute Engine instances. With an awareness of virtual machine adds, moves, or deletes within a Google VPC, you can create security policy rules that automatically adapt to changes in your application environment.

When Stackdriver is enabled, the firewall can retrieve metadata on eight predefined attributes—hostname of the VM, machine type, status (running or not), source (OS type), VPC Network, subnetwork, zone, and Project ID. In addition to these attributes, you can retrieve up to 24 user-defined attributes such as labels, tags, and other key-value pairs defined using metadata or startup scripts on the Google Compute Engine instances.

**STEP 1** | Select **Device > VM Information Sources**, and **Add** a new source to monitor.

**STEP 2** | Enter a unique **Name** for the source.

**STEP 3** | Select the **Service Authentication Type**.

- **VM-Series running in GCE**—Use this option if a VM-Series firewall deployed on GCE is monitoring the virtual machines on GCE. You do not need to provide account credentials if the service account that you used to provision the firewall has the permissions required to authenticate to the Google Cloud Project you want to monitor.
- **Service Account**—Use this option on any hardware-based firewall or VM-Series firewall that is not running on GCE. You must provide the **Service Account Credential** as a JSON file so that the firewall can authenticate to the GCP infrastructure and retrieve the attributes.

**STEP 4** | Enter the **Project ID** and the **Zone** in which the resources are deployed.

**STEP 5** | Click **OK** and **Commit** your changes.

**STEP 6** | Verify the connection **Status** is successful and that the firewall is able to connect to the GCE project you want to monitor.

**STEP 7** | Use the attributes as match criteria in **dynamic address groups**.
Enable VM-Series Firewall to Track Changes on Google Cloud Platform VMs

You can also enable any firewall that runs PAN-OS 8.1 (virtual or physical) to monitor application workloads deployed on Google Compute Engine instances. For a description of the PAN-OS metrics that you can publish to Google Stackdriver, see Custom PAN-OS Metrics Published for Monitoring.

**STEP 1 |** Push PAN-OS metrics from a VM-Series firewall on a Google Compute Engine instance to Stackdriver.

1. Log in to the web interface on the VM-Series firewall.
2. Select **Device > Operations.** On the Google Cloud Stackdriver Monitoring Setup panel, click **Edit.**
   1. Check **Publish PAN-OS metrics to Stackdriver.**
   2. Set **Update Interval** to a value between 1-60 minutes. This is the frequency at which the firewall publishes the metrics to Stackdriver. The default is 5 minutes.
   3. Click **OK.**
   4. **Commit** the changes.

   Wait until the firewall starts to publish metrics to Stackdriver before you configure alarms for PAN-OS metrics.

**STEP 2 |** Verify that you can see the metrics on Stackdriver.

1. In the Google Cloud Console, select **Products and Services > Monitoring.**
2. In Stackdriver, choose **Resources > Metrics Explorer.**
3. Under "Find resource type and metric", click in the search field and type **custom** to filter the PAN-OS metrics.
STEP 3 | Configure alerts and actions for PAN-OS metrics on Stackdriver. See Monitoring Quickstart for Google Compute Engine, and Stackdriver Introduction to Alerting.
Decryption Features

- Decryption Broker
- Automatic SAN Support for SSL Decryption
- HSM Client Upgrade and SafeNet HSM Cluster Support
- ECDSA Certificate Support for SSL Decryption with HSMs
- Decryption Port Mirroring Support Extension
Decryption Broker

Offload SSL decryption to the Palo Alto Networks firewall and decrypt traffic only once. A firewall enabled as a decryption broker forwards clear text traffic to security chains (sets of inline, third-party appliances) for additional enforcement. This allows you to consolidate security functions on the firewall, optimize network performance, and reduce the number of devices in your security infrastructure.

A decryption broker firewall uses a pair of designated forwarding interfaces to connect to the security chain. Together, the firewall and the security chain function as private analysis network—the clear text traffic flowing through this network is totally segmented from dataplane traffic. The decryption broker firewall first inspects the decrypted (now clear text) SSL traffic, and then sends it to the security chain. If you’ve configured multiple security chains, the firewall can perform session distribution to avoid oversubscribing any one chain. Then, last device in a security chain sends the clear text traffic back to the firewall. The firewall re-encrypts the traffic and sends it to its destination.

How you deploy decryption broker might vary depending on what type of security chain you plan to use. Two types of security chain deployments are supported: Layer 3 security chains (devices have assigned IP addresses and are configured with static routes to direct traffic) and transparent bridge security chains (devices do not have IP addresses or local routing tables and are serially connected).

Decryption broker is supported for PA-7000 Series, PA-3200 Series, PA-5200 Series, and VM-Series devices, and is supported only for outbound SSL traffic (from internal users to the internet) that is being decrypted using SSL Forward Proxy decryption. To learn more about decryption broker, and for detailed and complete steps to enable this feature, see Decryption Broker. Enabling decryption broker includes:

- Deciding what security chain deployment to use—a Layer 3 security chain or a Transparent Bridge security chain—and follow the guidelines to configure that security chain.
- Activating the free Decryption Broker license.
- Confirming that SSL Forward Proxy decryption is enabled.
- Enabling the firewall to act as a decryption broker with a Layer 3 security chain or a Transparent Bridge security chain. This includes designating a pair of Layer 3 interfaces to connect the firewall to the security chain, and optionally configuring the firewall to forward to multiple security chains.
Automatic SAN Support for SSL Decryption

Some browsers require server certificates to use a Subject Alternative Name (SAN) to specify the domains the certificate protects, and no longer support certificate matching based on a server certificate Common Name (CN). SANs enable a single server certificate to protect multiple names; CNs are less well-defined than SANs and can protect only a single domain or all first-level subdomains on a domain. However, if a server certificate contains only a CN, browsers that require a SAN will not allow end users to connect to the requested web resource.

Now, the firewall can add a SAN to the impersonation certificate it generates to establish itself as a trusted third-party during SSL decryption. When a server certificate contains only a CN, a firewall performing SSL decryption copies the server certificate CN to the impersonation certificate SAN. The firewall presents the impersonation certificate with the SAN to the client, and the browser is able to support the connection. End users can continue to access the resources they need, and the firewall can decrypt the sessions.

**STEP 1** | To decrypt and inspect SSL/TLS traffic from internal users to the web, configure SSL Forward Proxy Decryption.

**STEP 2** | Enable the firewall to add a SAN to impersonation certificates.

1. Select Objects > Decryption Profile and Add or modify a profile.
2. Select SSL Decryption > SSL Forward Proxy and then enable the firewall to Append certificate's CN value to SAN extension

**STEP 3** | Attach the updated Decryption profile to a Decryption policy to enforce the new setting on matching traffic (Policies > Decryption > Options > Decryption Profile).
HSM Client Upgrade and SafeNet HSM Cluster Support

When you use your firewall as a hardware security module (HSM) client to manage your digital keys, that firewall HSM client can run SafeNet client versions 5.4.2 and 6.2.2 and Thales nShield client version 12.30. These newer HSM client versions provide necessary compatibility with newer HSM server versions. Refer to the HSM vendor documentation for the client-server compatibility matrix and for any upgrade/downgrade considerations.

It is possible that downgrading an HSM server won’t be an option after you upgrade it. See HSM Client Upgrade and SafeNet HSM Cluster Support in Upgrade/Downgrade Considerations.

Thales nShield client—Your firewall is automatically upgraded from client version 11.62 to 12.30 in PAN-OS® 8.1. The firewall HSM client can support up to two independent Thales HSM servers.

SafeNet HSM client—Use the following information and task to configure your firewall as needed.

View the current running HSM client version by selecting Device > Setup > HSM and then Select HSM Client Version (in the Hardware Security Operations window). When you upgrade from a PAN-OS 8.0 release to PAN-OS 8.1, the firewall will use a specific SafeNet client version as follows:

- If your PAN-OS 8.0 release uses SafeNet client version 5.2.1, upgrading to PAN-OS 8.1 results in the firewall using SafeNet client version 5.4.2.
- If your PAN-OS 8.0.2 or later PAN-OS 8.0 release uses SafeNet client version 5.4.2 or 6.2.2, upgrading to PAN-OS 8.1 results in the firewall using the same SafeNet client version it was using before the upgrade. If the firewall was using SafeNet client version 5.4.2 and you want to install SafeNet client version 6.2.2, you can perform the task below after you upgrade to PAN-OS 8.1.

Additionally, the number of SafeNet HSM servers supported in a high availability (HA) configuration is enhanced from an HA pair of HSMs (two) to a cluster of up to 16 HSMs. However, the HSM servers in the cluster must all run the same SafeNet version and must authenticate separately. Use a SafeNet HSM cluster only when you need to replicate the keys across the cluster. Alternatively, you can add up to 16 SafeNet HSM servers that function independently.

HSM client integration is supported on Panorama and all firewall models except for PA-800 Series, PA-500, PA-220, PA-220-R, and PA-200 firewalls.

**STEP 1** | Install the SafeNet Client RPM Packet Manager as described when you Set Up Connectivity with an HSM.

**STEP 2** | Set up connectivity with SafeNet HSM servers as described when you Set Up Connectivity with a SafeNet Network HSM. You can establish HA with a cluster of up to 16 HSM servers.
ECDSA Certificate Support for SSL Decryption with HSMs

If you use Elliptic Curve Digital Signature Algorithm (ECDSA) certificates for SSL decryption, you can now securely store your elliptic curve private keys on a third-party network HSM. This means the firewall can import or generate an ECDSA certificate when you enable the **Private key resides on Hardware Security Module** option so that the firewall can get the ECDSA key from the HSM to decrypt traffic between a client and server. Prior to PAN-OS 8.1, you could not store ECDSA certificates on an HSM.

HSM support for ECDSA certificates applies to SSL decryption in both forward proxy and inbound inspection modes.

At the start of a TLS handshake, the firewall checks the HSM connection. If the HSM connection fails at the start of a session, the firewall blocks or allows the session depending on whether you enabled the **Block session if HSM not available** option. However, when the HSM connection fails in the middle of a session, the firewall will block the session.
Decryption Port Mirroring Support Extension

Support for decryption port mirroring is now available on all hardware-based firewalls and VM-Series firewall models. Decryption port mirroring allows you to copy decrypted traffic from a firewall and then send it to a traffic collection tool, such as NetWitness or Solera. Decryption mirroring requires a Decryption Port Mirror license. This license is free of change and you can activate it through the customer support portal.

This feature is not supported on the VM-Series firewall on VMware NSX and public cloud hypervisors (Amazon Web Services, Microsoft Azure, and Google Cloud Platform).
Panorama Features

> Device Monitoring on Panorama
> Configuration Reusability for Templates and Template Stacks
> Panorama Virtual Appliance and Virtual Dedicated Log Collector on AWS
> Panorama Virtual Appliance and Virtual Dedicated Log Collector on AWS GovCloud on page 71
> Panorama Virtual Appliance and Virtual Dedicated Log Collector on Azure
> Panorama Virtual Appliance and Virtual Dedicated Log Collector on Google Cloud Platform
> Panorama Virtual Appliance and Virtual Dedicated Log Collector on KVM on page 76
> Panorama Virtual Appliance and Virtual Dedicated Log Collector on Hyper-V on page 78
> Virtual Dedicated Log Collector on ESXi
> Streamlined Panorama Deployment for Application and Threat Content Updates
> Content Update Revert from Panorama
> Direct Query of PA-7000 Series Firewalls from Panorama
> Panorama Interconnect on page 85
Device Monitoring on Panorama

Now you can display the health information (Panorama > Managed Devices > Health) or the summary information (Panorama > Managed Devices > Summary) for your managed firewalls. You must upgrade both Panorama™ and firewalls to PAN-OS 8.1 before you can monitor the summary session, logging, resource, and environmental performance for managed firewalls in the summary. You can view the time-trended graphs and tables for the device sessions, environmental metrics, interfaces, logging, resources, and high availability performance for selected devices. Panorama calculates the baseline performance for each metric using seven-day averages and standard deviations to determine a normal operating range for the specific firewall. You can identify firewalls experiencing performance-related issues by viewing Panorama > Managed Devices > Health > Deviating Devices to isolate issues before they can seriously impact your business. When Panorama identifies a metric that is outside the normal operating range, the metric is marked and the firewall populates the Deviating Devices tab. For more information, see Monitor Device Health.

1 Managed Devices is now split into two sections:
   - **Summary**—Displays summary information about firewalls managed by the Panorama. The same summary information is shown here as in previous releases.
   - **Health (New)**—Displays the health status of all healthy firewalls and all firewalls outside normal operating range (Deviating Devices). Selecting a firewall takes you to the Detailed Device View where you can view the time-trended graphs and tables of monitored metrics.

2 View All Devices for a list of all managed firewalls regardless of device health status.

3 View the Deviating Devices for a list of all firewalls that are reporting metrics of the calculated baseline. Metrics that deviate outside the calculated baselines appear in red text:
Device Monitoring on Panorama

![Device Monitoring on Panorama Diagram]

| Device Name | Management Plane  | Logging Rate (logpm)
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CPU (%)</td>
<td>MEM (%)</td>
</tr>
<tr>
<td>unifi-branch3</td>
<td>30</td>
<td>20</td>
</tr>
<tr>
<td>PA-1x2</td>
<td>14</td>
<td>29</td>
</tr>
<tr>
<td>site-branch4</td>
<td>2</td>
<td>45</td>
</tr>
</tbody>
</table>
Configuration Reusability for Templates and Template Stacks

Templates and template stacks are improved to make it easier to manage firewalls and appliances from Panorama™ using a single template or template stack. To more easily reuse templates and template stacks, you can now create template variables in place of firewall-specific and appliance-specific IP literals in your configurations. You can define template variables at either the template level or the template stack level and you can use them to replace IP addresses, IP ranges, FQDNs, group IDs, and interfaces in IKE, VPN and HA configurations. You can override variables associated with and managed by the template or template stack on a per-firewall or appliance basis. Overriding a template or template stack variable allows you to minimize the number of templates and template stacks you need to manage while still allowing you to keep any device-specific configurations as needed. To reduce the number template and template stack configurations you need to manage, you now add firewalls and appliances to a template stack rather than to a template; the firewall or appliance prioritizes the template stack configuration. Additionally, template stacks can now reference any named object in a template that belongs to the template stack, which means you use template stacks to manage the base firewall and appliance configurations while template configurations enable you to create specific configurations. For more information, see Configure a Template or Template Stack Variables and Manage Templates and Template Stacks.

To create a template variable:

**STEP 1** Create a template and template stack using a variable name for an object. Variable names must start with the dollar sign ("$") symbol. For example, you could use $Panorama as a variable for the Panorama IP address that you want to configure on multiple managed firewalls and appliances.

1. Add a Template.
2. Configure a Template Stack.

**STEP 2** In Panorama > Templates, click Manage (Variables column).

**STEP 3** Add a new variable.
Variables can also be created inline where variables are supported.

**STEP 4** | **Commit and Push** the configuration changes to the managed firewalls and appliances.

**STEP 5** | Verify that the variables were pushed to the managed firewalls and appliances. Values defined by a variable display a variable symbol (-variable symbol) and you can hover over the symbol to view the template or template stack to which the variable definition belongs. A variable that is overridden displays an overridden variable symbol (variable symbol).
Panorama Virtual Appliance and Virtual Dedicated Log Collector on AWS

Panorama™ continues to expand the number of supported virtual environments to help reduce your physical footprint and giving you more flexibility when deploying your Palo Alto Networks® management and log collection services alongside other applications you deployed on Amazon® Web Services (AWS®). The Panorama virtual appliance on AWS supports all deployment modes (Panorama, Log Collector, and Management) and each mode shares the same processes and functionality as its M-Series counterpart. Refer to Panorama Models for more information on Panorama modes.

For more information, see Install Panorama on AWS.

STEP 1 | Log in to the Amazon Web Service Console and select the EC2 dashboard.

STEP 2 | Set up the VPC for your network needs.

STEP 3 | Deploy Panorama on Amazon Web Services.
1. On the EC2 Dashboard, Launch Instance and then select My AMIs and Select the Panorama 8.1.0 AMI.
2. Launch the Panorama virtual appliance as an EC2 instance.
   1. Choose the EC2 instance type for allocating the resources required for the Panorama virtual appliance, and click Next: Configure Instance Details. See the Setup Prerequisites for the Panorama VirtualAppliance for resource requirements.
   2. Select the VPC.
   3. Select the public subnet for the Panorama virtual appliance management interface.
   4. Automatically assign a public IP address.
   5. Click Next: Add Storage and Add New Volume to add log storage.
   6. (Optional) Add one or more tags as metadata to help you identify and group the Panorama virtual appliance. For example, add a Name tag with a Value that helps you identify which firewalls the Panorama virtual appliance manages.
   7. Create a new Security Group or select an existing one with—at minimum—HTTPS and SSH enabled
   8. Review and Launch and then verify that your selections are accurate before you Launch.
   9. Select an existing key pair or create a new one and acknowledge the disclaimer.

As a best practice, create a new key for each instance of Panorama or Dedicated Log Collector on AWS.

10. If you create a new key, download and save the private key to a safe location; the file extension is .pem. You cannot regenerate this key if it is lost.

   It takes 20 to 30 minutes to launch the Panorama virtual appliance using the minimum requirements.

STEP 4 | Enable management access to the Panorama virtual appliance.
1. Shut down the Panorama virtual appliance.
2. Create virtual network interfaces as needed and attach the interfaces to the Panorama virtual appliance. The virtual network interfaces are called Elastic Network Interfaces (ENIs) on AWS. You use these interfaces to manage devices from the virtual appliance.
The Panorama virtual appliance on AWS supports a single management interface; you must use this interface for log collection and device management.

3. Create or assign an Elastic IP (EIP) address to the management interface.

**STEP 5 |** Configure a new administrative password for the Panorama virtual appliance.

You must configure a unique administrative password before you can access the web interface of the Panorama virtual appliance. The private key you used to launch the Panorama virtual appliance is required to access the CLI.

**STEP 6 |** Activate the licenses on the Panorama virtual appliance.

**STEP 7 |** Finish configuring the Panorama virtual appliance for your deployment needs.

- *(Management Only mode)* Set Up a Panorama Virtual Appliance in Management Only Mode.
- *(Log Collector mode)* Skip to Step 6 to set up the Panorama virtual appliance as a Log Collector.

> When configuring the Management interface in Step 9, enter the Public IP Address of the Dedicated Log Collector. You cannot specify the IP Address, Netmask, or Gateway.

- *(Panorama and Management Only mode)* Configure a Managed Collector. Manage a Dedicated Log Collector from the Panorama virtual appliance for log collection of managed firewalls.
Panorama Virtual Appliance and Virtual Dedicated Log Collector on AWS GovCloud

Panorama continues to expand supported virtual environments to help reduce your physical footprint by giving you more flexibility in deploying your Palo Alto Networks management and log collection services along side other application you have deployed on Amazon Web Services. The Panorama virtual appliance on AWS supports all deployment modes (Panorama, Log Collector, and Management) and share the same processes and functionality as their M-Series counterparts. Refer to Panorama Models for more information on the Panorama modes.

For more information, see Install Panorama on AWS GovCloud.

STEP 1 | Log in to the AWS GovCloud Web Service Console and select the EC2 dashboard.

STEP 2 | Set up the VPC for your network needs.

STEP 3 | Deploy Panorama on Amazon Web Services.

1. On the EC2 Dashboard, click Launch Instance and then select My AMIs and Select the Panorama 8.1.0 AMI.
2. Launch the Panorama virtual appliance as an EC2 instance.
   1. Choose the EC2 instance type for allocating the resources required for the Panorama virtual appliance, and click Next: Configure Instance Details. See the Setup Prerequisites for the Panorama Virtual Appliance for resource requirements.
   2. Select the VPC.
   3. Select the public subnet for the Panorama virtual appliance management interface.
   4. Select Automatically assign a public IP address.
   5. Click Next: Add Storage and Add New Volume to add log storage.
   6. (Optional) Add one or more tags as metadata to help you identify and group the Panorama virtual appliance. For example, add a Name tag with a Value that helps you identify which firewalls the Panorama virtual appliance manages.
   7. Create a new Security Group or select an existing one with HTTPS and SSH enabled at a minimum.
   8. Select Review and Launch and verify that your selections are accurate before you select Launch.
   9. Select an existing key pair or create a new one and acknowledge the disclaimer.

As a best practice, create a new key for each instance of Panorama or Dedicated Log Collector on AWS.

10. If you created a new key, download and save the private key to a safe location; the file extension is .pem. You cannot regenerate this key if lost.
    It takes 20-30 minutes to launch the Panorama virtual appliance using the minimum requirements.

STEP 4 | Enable management access to the Panorama virtual appliance.

1. Shut down the Panorama virtual appliance.
2. Create virtual network interface(s) and attach the interface(s) to the Panorama virtual appliance. The virtual network interfaces are called Elastic Network Interfaces (ENIs) on AWS. These interfaces are used for managing devices from the virtual appliance.
   The Panorama virtual appliance on AWS supports a single management interface. You must use this interface for log collection and device management.
3. Create or assign an Elastic IP (EIP) address to the management interface.

**STEP 5 |** Configure a new administrative password for the Panorama virtual appliance.

You must configure a unique administrative password before you can access the web interface of the Panorama virtual appliance. To access the CLI, the private key used to launch the Panorama virtual appliance is required.

**STEP 6 |** Activate the licenses on the Panorama virtual appliance.

**STEP 7 |** Complete configuring the Panorama virtual appliance for your deployment needs.

- **(Management Only mode)** Set Up a Panorama Virtual Appliance in Management Only Mode.
- **(Log Collector mode)** Begin at Step 6 to set up the Panorama virtual appliance as a Log Collector.

> When configuring the Management interface in Step 9.3, enter the Public IP Address of the Dedicated Log Collector. You do not have the option to enter the IP Address, Netmask, or Gateway.

- **(Panorama and Management Only mode)** Configure a Managed Collector. Manage a Dedicated Log Collector from the Panorama virtual appliance for log collection of managed firewalls.
Panorama Virtual Appliance and Virtual Dedicated Log Collector on Azure

You can now deploy Panorama™ and a Dedicated Log Collector on Microsoft® Azure®. The Panorama virtual appliance on Azure supports all deployment modes (Panorama, Log Collector, and Management Only) and each mode shares the same processes and functionality as its M-Series counterpart. Refer to Panorama Models for more information on Panorama modes.

For more information, see Install Panorama on Azure.

STEP 1 | Log in to the Microsoft Azure portal.

STEP 2 | Deploy the Panorama virtual appliance.

1. In the Azure Dashboard, select Virtual machines, Add a VM, search for Panorama (BYOL), and Create the Panorama virtual appliance.
2. Configure the basic settings for the Panorama virtual appliance.
3. Configure the Panorama virtual appliance size. Refer to the Setup Prerequisites for the Panorama Virtual Appliance for sizing requirements. The Panorama virtual appliance defaults to Management Mode if you do not configure it to meet the minimum requirements for Panorama or Log Collector mode.
4. Configure storage and networking.
   The Panorama virtual appliance on Azure supports a single management interface. You must use this interface for log collection and device management.
5. Review the summary, accept the terms of use and privacy policy, and then Create (deploy) the Panorama virtual appliance.
6. Verify that you have successfully deployed the Panorama virtual appliance.

   It takes 20 to 30 minutes to launch the Panorama virtual appliance and can take longer depending on the resources you configured for the virtual machine. ICMP protocol is not permitted by Microsoft Azure so you cannot ping the Panorama virtual appliance to determine whether it is successfully deployed.

STEP 3 | Log in to the web interface of the Panorama virtual appliance.

STEP 4 | Activate the licenses on the Panorama virtual appliance.

STEP 5 | Finish configuring the Panorama virtual appliance for your deployment needs.

   • (Management Only mode) Set Up a Panorama Virtual Appliance in Management Only Mode.
   • (Log Collector mode) Skip to Step 6 to set up the Panorama virtual appliance as a Log Collector.

   When configuring the Management interface in Step 9, enter the Public IP Address of the Dedicated Log Collector. You cannot specify IP Address, Netmask, or Gateway.

   • (Panorama and Management Only mode) Configure a Managed Collector. Manage a Dedicated Log Collector from the Panorama virtual appliance for log collection of managed firewalls.
Panorama Virtual Appliance and Virtual Dedicated Log Collector on Google Cloud Platform

You can now deploy Panorama™ and a Dedicated Log Collector on Google® Cloud Platform (GCP™). The Panorama virtual appliance on GCP supports all deployment modes (Panorama, Log Collector, and Management Only) and each mode shares the same processes and functionality as its M-Series counterpart. Refer to Panorama Models for more information on Panorama modes. Panorama virtual appliance and virtual Dedicated Log Collector on GCP is available only on PAN-OS 8.1.1 and later releases.

For more information, see Install Panorama on Google Cloud Platform.

STEP 1 | Download the Panorama virtual appliance image.
1. Log in to the Palo Alto Networks Support Portal.
2. Select Updates > Software Updates and filter by Panorama Base Images.
3. Download the latest version of the Panorama on GCP tar.gz image.

STEP 2 | Upload the Panorama virtual appliance image to the Google Cloud Platform.
1. Log in to the Google Cloud Console.
2. From the Products and Services menu, select Storage.
3. Click Create Bucket, configure the new storage bucket and click Create.
4. Select the storage bucket you created in the previous step, click Upload files, and select the Panorama virtual appliance image you downloaded.
5. From the Products and Services menu, select Compute Engine > Images.
6. Click Create Image and create the Panorama virtual appliance image:
   1. Name the Panorama virtual appliance image.
   2. In the Source field, select Cloud Storage file from the drop-down menu.
   3. Click Browse and navigate to the storage bucket where you uploaded the Panorama virtual appliance image, and Select the uploaded image.
   4. Create the Panorama virtual appliance image.

STEP 3 | Configure the Panorama virtual appliance.
1. From the Products and Services menu and select the Compute Engine.
2. Click Create Instance to begin deploying the Panorama virtual appliance.
3. Add a descriptive Name to easily identify the Panorama virtual appliance.
4. Select the Zone where you want to deploy the Panorama virtual appliance.
5. Allocate the Machine Type CPU cores and memory. Refer to the Setup Prerequisites for the Panorama Virtual Appliance for minimum resource requirements.
6. For the Boot Disk, click Change > Custom image, select the Panorama image file you uploaded in Step 2, and click Select.
7. Under Identity and API access, Allow full access to all Cloud APIs.
8. Under Firewall, Allow HTTPS traffic.

STEP 4 | Enable management access to the Panorama virtual appliance.
1. Expand Management, disks, networking SSH keys.
2. Enable access to the serial port so you can manage the Panorama virtual appliance.
3. Configure the management interface on the Panorama virtual appliance.

To learn more about how to reserve IP addresses, refer to the information about how to Reserve a Static Internal IP Address and how to Reserve a Static External IP Address.

The Panorama virtual appliance on GCP supports a single management interface; you must use this interface for log collection and device management.

4. Configure the SSH key. You need an SSH key to access the Panorama virtual appliance CLI to configure the administrative user password after initial deployment.

STEP 5 | (Panorama and Log Collector mode) Add additional storage for log collection. Repeat this step as needed to add additional virtual logging disks.

If you intend to use the Panorama virtual appliance in Panorama mode or as a Dedicated Log Collector, add the virtual logging disks during the initial deployment. By default, the Panorama virtual appliance is in Panorama mode for the initial deployment when you meet the Panorama mode resource requirements and you have added at least one virtual logging disk. Otherwise, the Panorama virtual appliance defaults to Management Only mode. Change the Panorama virtual appliance to Management Only mode if you need to only manage devices and Dedicated Log Collectors and you don’t need to collect logs locally.

The Panorama virtual appliance on GCP supports only 2TB logging disks and, in total, supports up to 24TB of log storage. You cannot add a logging disk smaller than 2TB or a logging disk with a size that is not evenly divisible by the 2TB logging disk requirement because the Panorama virtual appliance partitions logging disks larger than 2TB into 2TB partitions.

STEP 6 | Create (deploy) the Panorama virtual appliance. The Panorama virtual appliances takes approximately 10 minutes to boot up after initial deployment.

STEP 7 | Configure a new administrative password for the Panorama virtual appliance.

Use a private key to access the CLI and configure a unique administrative password so that you can access the web interface of the Panorama virtual appliance.

STEP 8 | Activate the licenses on the Panorama virtual appliance.

STEP 9 | Finish configuring the Panorama virtual appliance for your deployment needs.

- (Management Only mode) Set Up a Panorama Virtual Appliance in Management Only Mode.
- (Log Collector mode) Skip to Step 6 to set up the Panorama virtual appliance as a Log Collector.

When configuring the Management interface in Step 9, enter the Public IP Address of the Dedicated Log Collector. You cannot specify IP Address, Netmask, or Gateway.

- (Panorama and Management Only mode) Configure a Managed Collector. Manage a Dedicated Log Collector from the Panorama virtual appliance for log collection of managed firewalls.
Panorama Virtual Appliance and Virtual Dedicated Log Collector on KVM

You can now deploy Panorama™ and a Dedicated Log Collector on KVM. The Panorama virtual appliance on KVM supports all deployment modes (Panorama, Log Collector, and Management Only) and each mode shares the same processes and functionality as its M-Series counterpart. Refer to Panorama Models for more information on Panorama modes. Panorama virtual appliance and virtual Dedicated Log Collector on KVM is available only on PAN-OS 8.1.2 and later releases.

For more information, see Install Panorama on KVM.

STEP 1 | Launch the Panorama virtual appliance.
1. Download the Panorama virtual appliance for KVM image.
2. Create a new virtual machine image and add the Panorama virtual appliance image for KVM to the Virtual Machine Manager.
3. Configure the Memory and CPU settings.
4. Name the Panorama virtual appliance, enable configuration customization, and select the management interface bridge.
   The Panorama virtual appliance on KVM supports a single management interface. You must use this interface for log collection and device management.
5. Configure the virtual system disk settings.
6. Configure the virtual machine console display to use the VNC server to interact with the virtual machine.
7. (Panorama and Log Collector mode) Add additional storage for log collection. Repeat this step as needed to add additional virtual logging disks.
   If you intend to use the Panorama virtual appliance in Panorama mode or as a Dedicated Log Collector, add the virtual logging disks during the initial deployment. By default, the Panorama virtual appliance is in Panorama mode for the initial deployment when you meet the Panorama mode resource requirements and you have added at least one virtual logging disk. Otherwise, the Panorama virtual appliance defaults to Management Only mode. Change the Panorama virtual appliance to Management Only mode if you need to only manage devices and Dedicated Log Collectors and you don’t need to collect logs locally.
   The Panorama virtual appliance on KVM supports only 2TB logging disks and, in total, supports up to 24TB of log storage. You cannot add a logging disk smaller than 2TB or a logging disk with a size that is not divisible by the 2TB logging disk requirement because the Panorama virtual appliance partitions logging disks larger than 2TB into 2TB partitions.
8. Begin Installation. The Panorama virtual appliances takes approximately 10 minutes to boot up.

STEP 2 | Configure the network access settings for the management interface.

STEP 3 | Activate the licenses on the Panorama virtual appliance.

STEP 4 | Finish configuring the Panorama virtual appliance for your deployment needs.
- (Management Only mode) Set Up a Panorama Virtual Appliance in Management Only Mode.
- (Log Collector mode) Skip to Step 6 to set up the Panorama virtual appliance as a Log Collector.

When configuring the Management interface in Step 9, enter the Public IP Address of the Dedicated Log Collector. You cannot specify IP Address, Netmask, or Gateway.
• **(Panorama and Management Only mode)** Configure a Managed Collector. Manage a Dedicated Log Collector from the Panorama virtual appliance for log collection of managed firewalls.
Panorama Virtual Appliance and Virtual Dedicated Log Collector on Hyper-V

Panorama continues to expand supported virtual environments to help reduce your physical footprint by giving you more flexibility in deploying your Palo Alto Networks management and log collection services along side other application you have deployed on Hyper-V. The Panorama virtual appliance on Hyper-V supports all deployment modes (Panorama, Log Collector, and Management) and share the same processes and functionality as their M-Series counterparts. Refer to Panorama Models for more information on the Panorama modes.

For more information, see Install Panorama on Hyper-V.

**STEP 1** | Download the VHDX file from the Palo Alto Networks Support Portal.

**STEP 2** | Set up any vSwitch(es) that you will need. For more information, review the Virtual Switch Types for more information.

**STEP 3** | Install the Panorama virtual appliance.

1. On the Hyper-V Manager, select the host and select **Action > New > Virtual Machine.** Configure the following settings in the New Virtual Machine Wizard:
   1. Choose a **Name** and **Location** for the Panorama virtual appliance. The Panorama virtual appliance stores the VHDX file at the specified location.
   2. Choose **Generation 1**. This is the default option and the only version supported.
   3. For **Startup Memory**, assign the memory based on the intended system mode. See the Setup Prerequisites for the Panorama Virtual Appliance for the memory requirements for each mode.

   **Do not enable dynamic memory; the Panorama virtual appliance requires static memory allocation.**

   4. Configure **Networking**. Select an external vSwitch to connect the management interface on the firewall.
   5. To connect the **Virtual Hard Disk**, select **Use an existing virtual hard disk** and browse to the VHDX file you downloaded earlier.
   6. Review the summary and click **Finish**.

**STEP 4** | Allocate the Panorama virtual appliance CPU cores.

Review the Setup Prerequisites for the Panorama Virtual Appliance for minimum resource requirements.

*If you plan to use the Panorama virtual appliance as a Dedicated Log Collector, ensure that you configure the appliance with the required resources during initial deployment. The Panorama virtual appliance does not remain in Log Collector mode if you resize the virtual machine after you deploy it, and this results in a loss of log data.*

1. In the **Hardware** list, select **Processor**.
2. Edit the currently allocated **Number of virtual processors**.

**STEP 5** | Connect at least one network adapter for the dataplane interface on the firewall. Repeat this to create additional network interfaces on the Panorama virtual appliance.

1. Select **Settings > Hardware > Add Hardware** and select the **Hardware type** for your network adapter.
Legacy Network Adapter and SR-IOV are not supported. If selected, the VM-Series firewall will boot into maintenance mode.

2. Click OK.

STEP 6 | (Panorama and Log Collector mode) Add additional storage for log collection. Repeat this step as needed to add additional virtual logging disks. If you want to deploy the Panorama virtual appliance in Management Only mode, continue to Step 7.

If you intend to use the Panorama virtual appliance in Panorama mode or as a Dedicated Log Collector, add the virtual logging disks during the initial deployment. By default, the Panorama virtual appliance is in Panorama mode for the initial deployment when you meet the Panorama mode resource requirements and have added at least one virtual logging disk.

The Panorama virtual appliance on Hyper-V only supports 2TB logging disks, and in total supports up to 24TB of log storage. You are unable to add a logging disk smaller than 2TB, or a logging disk with a size not divisible by the 2TB logging disk requirement. The Panorama virtual appliance partitions logging disks larger than 2TB into 2TB partitions.

1. On the Hyper-V Manager, select the host and select Action > New > Hard Disk.
2. If you see the Before You Begin prompt, click Next to begin adding the virtual logging disk.
3. For the Disk Format, select VHDX. Click Next to continue.
4. For the Disk Type, select Fixed Size or Dynamically Expanding based on your needs. Click Next to continue.
5. Specify the Name and Location for the virtual logging disk file. Click Next to continue.
6. To configure the disk, select Create a new virtual hard disk and enter the disk size. Click Next to continue.
7. Review the Summary and Finish adding the virtual hard logging disk.

STEP 7 | Power on the Panorama virtual appliance.

STEP 8 | Configure the IP address of the management interface.

STEP 9 | Configure a new administrative password for the Panorama virtual appliance.

You must configure a unique administrative password before you can access the web interface of the Panorama virtual appliance. To access the CLI, the private key used to launch the Panorama virtual appliance is required.

STEP 10 | Activate the licenses on the Panorama virtual appliance.

STEP 11 | Complete configuring the Panorama virtual appliance for your deployment needs.

- (Management Only mode) Set Up a Panorama Virtual Appliance in Management Only Mode.
- (Log Collector mode) Begin at Step 6 to set up the Panorama virtual appliance as a Log Collector.

When configuring the Management interface in Step 9.3, enter the Public IP Address of the Dedicated Log Collector. You do not have the option to enter the IP Address, Netmask, or Gateway.

- (Panorama and Management Only mode) Configure a Managed Collector. Manage a Dedicated Log Collector from the Panorama virtual appliance for log collection of managed firewalls.
Virtual Dedicated Log Collector on ESXi

Panorama continues to expand supported virtual environments to help reduce your physical footprint by giving you more flexibility in deploying your Palo Alto Networks management and log collection services along side other application you have deployed on the ESXi hypervisor. The Panorama virtual appliance deployed as a Dedicated Log Collector on ESXi supports all deployment modes share the same processes and functionality as their M-Series counterparts. For more information, see Set Up the M-Series Appliance as a Dedicated Log Collector.

**STEP 1 |** Install Panorama on an ESXi server.

**STEP 2 |** Switch from Panorama mode to Log Collector mode on each Panorama virtual appliance to set up a Dedicated Log Collector.

**STEP 3 |** Record the serial number of the Log Collector. You will need the serial number to add the Log Collector as a managed collector.

**STEP 4 |** Add the Log Collector as a managed collector on the Panorama management server.

**STEP 5 |** Enable the logging disks.
Streamlined Panorama Deployment for Application and Threat Content Updates

When using Panorama to deploy content updates to managed firewalls, you can now more easily configure dynamic updates schedules for multiple firewalls at once based on platform, device group, and tag (instead of applying schedules based on individual firewall serial numbers, as was previously supported). If yours is a mission-critical network, this is especially useful to stagger content updates across your network and to enforce content update installation threshold. A content update installation threshold only allows firewalls to install Applications and Threat content updates that have been successfully functioning in customer environments for a given amount of time, and a separate installation threshold for content updates with new App-IDs gives you extra time to assess how new application signatures impact your security policy. Previously, you could only use Panorama to configure content updates thresholds for managed firewalls that were connecting to the Palo Alto Networks Update Server directly, not those firewalls that retrieve content updates from Panorama.

For guidance on how to best deploy Application and Threat content updates based on your organization’s network security and application availability requirements, review the Best Practices for Application and Threat Content Updates. Then, to easily apply a Dynamic Updates Schedule to several devices at once, and to set a Content Update Threshold for those devices, start by editing or adding a Dynamic Updates schedule for managed firewalls:

STEP 1 | Select Panorama > Device Deployment > Dynamic Updates > Schedules.

STEP 2 | Set the schedule Type to App and Threat.

STEP 3 | Set the schedule Action to Download and Install.

STEP 4 | Use Filters to set a Dynamic Updates schedule for many devices at once based on Platforms, Device Groups, and Tags.

STEP 5 | Set a Threshold requirement for new Applications and Threat content releases—managed firewalls only retrieve and install content releases from Panorama that have been available and functioning in customer environments for at least the amount of time that you define.
You can quickly revert the Applications, Applications and Threats, Antivirus, WildFire®, and WildFire™ content versions of one or more firewalls, Log Collectors, or WildFire appliances directly from Panorama™.

Using Panorama to revert content versions installed on managed firewalls and appliances provides a centralized workflow that helps mitigate risks associated with new or modified applications or new threat signatures that are introduced in a content update. The ability to revert content release versions on one or more managed firewalls or appliances from Panorama allows you to quickly revert a content update (such as one that adversely affected your network operations and security) from a single location rather than having to access and revert content updates for one managed firewall or appliance at a time. Additionally, for each firewall and appliance you revert, Panorama generates a system log. For more information, see the Best Practices for Content and Threat Content Updates before you deploy content updates to your managed firewalls and appliances.

**STEP 1 |** Log in to the Panorama Web Interface.

**STEP 2 |** Select Panorama > Device Deployment > Dynamic Updates and Revert Content.

**STEP 3 |** Select the content update type you need to revert.

**STEP 4 |** Select one or more firewalls or appliances on which you need to revert content and click OK. The content version you revert to must be an earlier version than the version currently installed on the firewall or appliance.
Direct Query of PA-7000 Series Firewalls from Panorama

Because PA-7000 Series firewall can now forward logs to Panorama, Panorama no longer treats the PA-7000 Series firewalls it manages as Log Collectors. If you have not configured the PA-7000 Series firewalls to forward logs to Panorama, all logs a managed PA-7000 Series firewall generates are only viewable from the local firewall and not from Panorama. If you do not yet have a log forwarding infrastructure that is capable of handling the logging rate and volume from the PA-7000 Series firewalls, you can now enable Panorama to directly query PA-7000 Series firewalls when monitoring logs.

For Panorama to directly query PA-7000 Series firewalls, the firewalls must be running PAN-OS 8.0.8 or later.

With this new functionality, Panorama now provides two options for monitoring logs and running reports for managed PA-7000 Series firewalls:

• **(New)** Enable Panorama to directly query managed PA-7000 Series firewalls when monitoring logs.

  To enable Panorama to directly query the PA-7000 Series firewalls without requiring the firewalls to forward logs, you must enter the following command from the Panorama CLI:

  ```
  admin@panorama> debug-reportd send-request-to-7k yes
  ```

  After running the command, you will be able to view logs for managed PA-7000 Series firewalls on the Panorama Monitor tab. Additionally, as with all managed devices, you can also generate reports that include PA-7000 Series log data by selecting Remote Device Data as the Data Source.

• **Configure the managed PA-7000 Series firewalls to forward logs to Panorama.**

  Before enabling your PA-7000 Series firewalls to forward logs to Panorama, make sure you have a logging infrastructure that will handle the logging rate and volume. Refer to the table in Panorama Models to determine if you have the right logging capacity. Additionally, if you have enabled Panorama to directly query PA-7000 Series firewalls, you must disable this before you enable log forwarding by entering the following command from the Panorama CLI:

  ```
  > debug-reportd send-request-to-7k no
  ```

  After you have enabled your PA-7000 Series firewalls to forward logs to Panorama, the PA-7000 Series log data will be aggregated within all Panorama views: Application Command Center (ACC), the App-Scope, the log viewer (Monitor tab), and the standard, customizable reporting options on Panorama.
Panorama Interconnect

The Panorama™ Interconnect plugin enables you to establish a Panorama Controller that manages Panorama Nodes and centralizes configuration management for consistent firewall configurations and policies across large-scale firewall deployments. This also helps reduce the time you spend synchronizing configurations on multiple Panorama management servers and improves the response time for security vulnerabilities in the event of a misconfiguration.

For more information, see Manage Large-Scale Firewall Deployments.

**STEP 1 | Set Up Panorama management servers** that shall function as the Controller and Nodes.

**STEP 2 | Install the Panorama Interconnect plugin.** You must install the plugin on the Panorama Controller and all Panorama Nodes.

1. Log in to the Panorama Web Interface.
2. Select Panorama > Plugins and search for Interconnect.
3. Download and Install the Panorama Interconnect plugin.
4. Click Commit > Commit to Panorama to finish installing the Panorama Interconnect plugin.

**STEP 3 | Enable Authentication Between the Panorama Controller and the Panorama Nodes.**

1. Obtain the certificate authority (CA) certificate for the Panorama Controller.
2. Generate the Panorama Node certificate.
3. Create a certificate profile for authenticating the Panorama Nodes.

**STEP 4 | Set Up the Panorama Interconnect Plugin.**

1. Set up the Panorama Controller. Repeat this step on the high availability (HA) peer if the Panorama Controller is in an HA configuration.

   After you configure the Panorama management server as the Panorama Controller, you cannot reconfigure that Controller as a Panorama Node. Verify that you are configuring the correct Panorama management server as the Panorama Controller before you continue to the next step.

   ![Setup](image)

2. Set up the Panorama Node. Repeat this step for all Panorama Nodes.

   ![Setup](image)

3. Add the Panorama Nodes to the Panorama Controller.

   ![Setup](image)
STEP 5 | Add a Device Group on the Panorama Controller.

STEP 6 | Configure a Template Stack on the Panorama Controller.

STEP 7 | Push the Common Panorama Configuration to Panorama Nodes.

STEP 8 | Synchronize the Panorama Node with the Panorama Controller.

STEP 9 | Add one or more firewalls to be managed by a Panorama Node.
   1. Add a Firewall to a Panorama Node.
   2. Import Multiple Firewalls to a Panorama Node.

STEP 10 | Push the Panorama Node Configuration to Managed Devices.
Content Inspection Features

- SCTP Security
- Rapid Deployment of the Latest Threat Prevention
- Tools to Avoid or Mitigate Content Update Issues
SCTP Security

Stream Control Transmission Protocol (SCTP) is a reliable message-based transport protocol (number 132) that sends multiple streams of signaling, voice, and other data simultaneously. Mobile networks use SCTP to transport signaling traffic on various interfaces, such as S1-MME, S6a, and X2.

You use the multilayered approach of your firewall to secure your SCTP traffic. You can filter SCTP traffic based on payload protocol IDs (PPIDs). You can apply granular-level filtering on Diameter traffic over SCTP and SS7 traffic over SCTP. You can validate SCTP packets to ensure they comply with RFC4960. You can also protect against flooding of SCTP initiation (INIT) packets. In the case of mobile networks, these SCTP security measures help to prevent attackers from causing network congestion and outages that disrupt data and voice services of mobile subscribers and IoT devices connected to these networks. Additionally, you can view SCTP logs, ACC information, and reports to verify configurations and gain visibility into the SCTP events and traffic between two endpoints.

Only PA-5200 Series and VM-Series firewall support SCTP security in PAN-OS 8.1 releases.

STEP 1 | Enable SCTP security.
2. Click OK.

STEP 2 | Create an SCTP Protection profile and specify the checks and filters you want to apply to SCTP traffic.
1. Add a profile by Name (Objects > Security Profiles > SCTP Protection).
2. Select SCTP Inspection to configure the action the firewall takes on unknown chunks, non-compliant chunks, and chunks of invalid length. Generating a log to alert you and blocking packets that have invalid chunks help you secure your SCTP traffic.

STEP 3 | Select the Log Settings for the profile—options to generate SCTP logs for allowed chunks, association start or end, and state failure events.

STEP 4 | Select Filtering Options for the profile so you can filter protocols running on top of SCTP.
1. Add SCTP filters to allow, block, or generate an alert for PPIDs.
2. Add Diameter filters to allow, block, or generate an alert for Diameter Application IDs, Command Codes, and Attribute/Value Pairs.
3. Add SS7 filters to allow, block, or generate an alert for SS7 chunks based on SCCP Calling Party SSN, SCCP Calling Party GT, and Operation Codes.

STEP 5 | Apply the SCTP Protection profile to a security policy rule.
2. Select Actions and in the Profile Setting section, select the SCTP Protection profile you created. Configure the rest of the Security policy rule and save it.

STEP 6 | Allocate SCTP log storage on the firewall if you want to capture SCTP logs.

Select Device > Setup > Management, edit the Logging and Reporting Settings, and select Log Storage. Enter quota percentages for SCTP, SCTP Summary, and the SCTP hourly, daily, and weekly summaries.

STEP 7 | View information about your SCTP traffic.
1. Select Monitor > Logs > SCTP to view the SCTP logs and detailed logs.
2. Select Monitor > Logs > Traffic and select the Detailed Log View (⁠🔍⁠) for a log where the Application is sctp to view a detailed traffic log for an SCTP association.

3. Select ACC > Mobile Network Activity to view SCTP events and association activity.

4. View predefined reports about SCTP events and errors by selecting Device > Setup > Management. Edit the Logging and Reporting Setting section and, for Predefined Reports, select any of the SCTP reports.

5. Create a custom report on SCTP events by selecting Monitor > Manage Custom Reports and adding a custom report that uses the SCTP database.
Rapid Deployment of the Latest Threat Prevention

The following two features enable you to quickly deploy the latest threat protections while ensuring availability for mission-critical applications:

- **New App-ID Threshold** on page 34—Fine tune content update installation thresholds so that threat updates install immediately as they’re released, and new App-IDs are installed only after you’ve had an opportunity to make any necessary security policy updates.

- **Streamlined Panorama Deployment for Application and Threat Content Updates**—Use Panorama to set an installation threshold for new App-IDs, and stagger the roll-out of new content to locations with less business risk first.
Tools to Avoid or Mitigate Content Update Issues

Palo Alto Networks Application and Threat Content Updates undergo rigorous performance and quality assurance; however, because there are so many possible variables in a customer environment, there are rare occasions where a content release might impact a network in a way that we did not foresee. The following features are intended to help both you and us avoid and mitigate an issue with a content release, so that there is as little impact to your network as possible.

Review the Best Practices for Application and Threat Content Updates for guidance on how to best deploy content updates based on your organization's network security and application availability needs.

- The firewall can now validate that a downloaded content update is still Palo Alto Networks-recommended at the time of installation.
  This check, which the firewall performs by default, is helpful in cases where content updates are downloaded from the Palo Alto Networks update server (either manually or on a schedule) ahead of installation. Because there are rare instances where Palo Alto Networks removes a content update from availability, this option prevents the firewall from installing a content update that Palo Alto Networks has deprecated, even if the firewall has already downloaded it.

- The threat intelligence telemetry data that the firewall sends to Palo Alto Networks now includes information that Palo Alto Networks can use to identify and troubleshoot issues with content updates.
  This new telemetry data helps us to quickly recognize a content update that is impacting firewall performance or security policy enforcement in unexpected ways, across the Palo Alto Networks customer base. We can quickly determine the firewall platforms or types of firewall deployments that are affected in order to help you to mitigate impact to your own network, or avoid the issue altogether.

  Make sure that you've enabled the firewall to collect and share telemetry data with Palo Alto Networks:
  1. Select Device > Setup > Telemetry.
  2. Edit the Telemetry settings and Select All.
  3. Click OK and Commit to save your changes.

- Palo Alto Networks can now directly alert you to a critical content release issue; we'll give you the information you need to understand if and how the issue affects you, along with steps to move forward.

  Palo Alto Networks can now issue alerts about content update issues directly to the firewall web interface or—if you have log forwarding enabled—to the external service you use for monitoring.

  In the firewall web interface, critical alerts about content issues are displayed similarly to the Message of the Day. When Palo Alto Networks issues a critical alert about a content update, the alert is displayed by default when you log into the firewall web interface. If you're already logged into the firewall web interface, you will notice an exclamation appear over the message icon on the menu bar located at the bottom of the web interface—click on the message icon to view the alert.

  Critical content update alerts are also logged as system log entries with the Type general and the event ID palo-alto-networks-message. Use the following filter to view these log entries: ( subtype eq dynamic-updates ) and ( eventid eq palo-alto-networks-message).
Set up **log forwarding** to send these entries to any external services that you use for monitoring network and firewall activity. This allows you to make sure that the appropriate personnel is notified when Palo Alto Networks issues an alert, so that they can take action as needed.

- After being notified about an issue with a content update, you can now use Panorama to revert managed firewalls to the last content update version, instead of manually reverting the content version for individual firewalls. To learn more, see [Content Update Reversion from Panorama](#).
Authentication Features

> Extensible Authentication Protocol (EAP) Support for RADIUS
> Authentication Using Custom Certificates for WildFire and PAN-DB
Extensible Authentication Protocol (EAP) Support for RADIUS

To securely transport administrator or end user credentials between RADIUS servers and the firewall, you can now use the following Extensible Authentication Protocols (EAP): PEAP-MSCHAPv2, PEAP with GTC, or EAP-TTLS with PAP.

The supported EAP methods create encrypted tunnels between the firewall and the RADIUS server to securely transmit usernames, passwords, and other credential information. The tunnel created by EAP consists of an inner tunnel and an outer tunnel. After the RADIUS server’s certificate is validated, the firewall creates the outer tunnel using SSL. After the encrypted TLS outer tunnel has been established, the firewall creates the inner tunnel to transmit the user’s credentials to the server.

To further protect user information from eavesdropping, you can mask the username by anonymizing the user’s identity in the outer tunnel. For authentication using GlobalProtect, you can optionally allow GlobalProtect users with expired passwords to successfully log in by permitting them to change their password.

You can use EAP with RADIUS to:
- Secure administrative access to the web interface on the firewall and Panorama
- Secure administrative access using CLI on the firewall and Panorama
- Authenticate end users through Captive Portal and GlobalProtect, including Clientless VPN and GlobalProtect Gateway

**STEP 1** | Add a Certificate Profile to allow the RADIUS server to authenticate with the firewall.
1. Install the Server Certificate and Key on the RADIUS server.
2. Add the hostname or IP address of the firewall as the RADIUS client.
3. Upload the Root-CA and Intermediate CA certificates used to sign the RADIUS server certificate on the firewall.

**STEP 2** | Create a RADIUS server profile that uses an EAP Authentication Protocol:
- **PEAP-MSCHAPv2 (Default)**—Protected EAP (PEAP) with Microsoft Challenge-Handshake Authentication Protocol (MSCHAPv2) provides improved security over PAP or CHAP by transmitting both the username and password in an encrypted tunnel. In addition, if you are using GlobalProtect, you can allow GlobalProtect users to change expired passwords.
- **PEAP with GTC**—Select Protected EAP (PEAPv0) with Generic Token Card (GTC) to use one-time tokens in an encrypted tunnel.
- **EAP-TTLS with PAP**—Select EAP with Tunneled Transport Layer Security and PAP to transport plaintext credentials for PAP in an encrypted tunnel.
The Auto option is no longer supported. For more information on changes to default behavior for this feature, see Changes to Default Behavior and Upgrade/Downgrade Considerations in the Release Notes.

STEP 3 | (Optional) Select whether GlobalProtect users can change expired passwords:
- **Allow users to change passwords after expiry** (PEAP-MSCHAPv2 with GlobalProtect only)—Select this option to allow GlobalProtect users to change expired passwords.
  
  *This feature is only supported with GlobalProtect client 4.1 or later.*

STEP 4 | Select whether the user’s identity is anonymous in the outer tunnel that the firewall creates to authenticate with the server:
- **Make Outer Identity Anonymous**—This option is enabled by default to anonymize the user’s identity in the outer tunnel, which is created after authenticating with the server.
  
  You must configure the RADIUS server to allow access for anonymous users. Some RADIUS server configurations may not support anonymous outer IDs, and you may need to clear the option. When cleared, usernames are transmitted using cleartext.
STEP 5 | Select the **Certificate Profile** that the server uses to authenticate the firewall.

STEP 6 | **Add** each RADIUS server.

STEP 7 | Select **Device > Authentication Profile, Add** a profile, and assign the RADIUS server profile to the authentication profile.

STEP 8 | To enable administrator access, select **Device > Setup > Management**, and select the **Authentication Profile**. Configure an Admin Role **profile** if the administrator uses a custom role and configure an access domain if the firewall has more than one virtual system.

STEP 9 | If you are using GlobalProtect, see **Enable Authentication Using an Authentication Profile**.

STEP 10 | If you are using Captive Portal, see **Map IP Addresses to Usernames Using Captive Portal**.

STEP 11 | **Commit** your changes to activate them on the firewall.

   To confirm the authentication is successful, use the `test authentication authentication-profile <auth-profile-name> username <username> password` command. You can also use the **Description** column in **Monitor > Authentication** to view the EAP outer and inner identities. To troubleshoot, use **grep** to search the logs for the number in the **Authentication ID** column. For more information, refer to the PAN-OS **Admin Guide**.
Authentication Using Custom Certificates for WildFire, PAN-DB, and Between Log Collectors

You can now configure mutual authentication between WildFire® or PAN-DB appliances and other Palo Alto Networks appliances using custom certificates. This allows you to establish a unique chain of trust between WildFire or PAN-DB and connected Palo Alto Networks appliances instead of relying on predefined certificates for inter-device communication. You can generate these certificates locally on Panorama or the firewall, obtain them from a trusted third-party certificate authority (CA), or obtain certificates from your own enterprise CA.

Additionally, you can configure mutual authentication between Log Collectors in a Collector Group. Local Log Collectors use the same client and server certificates as Panorama.

You can configure the client certificate and certificate profile on each client device or push the configuration from Panorama to each device as part of a template.

This feature is an extension of Authentication Using Custom Certificates introduced in PAN-OS 8.0.

- Custom certificates for a standalone WildFire appliance or a PAN-DB appliance—You can deploy custom certificates between a WildFire or PAN-DN appliance that receives samples or URL information from a firewall. In this case, the firewall acts as the client and the WildFire appliance or PAN-DB appliance acts as the server. Use the CLI to deploy custom certificates directly on the WildFire appliance or PAN-DB appliance.
- Custom certificate for a WildFire appliance managed by Panorama—This allows you to configure custom certificate communication between WildFire appliance that receives samples from firewalls. In this deployment, the WildFire appliance is the server and the firewalls are the clients. However, you can complete the server and client communication configuration through the Panorama web interface instead of the WildFire appliance CLI.
- Custom certificates for a WildFire appliance as a client—You can deploy custom certificates for the communication channel Panorama uses to push configuration information to a WildFire appliance. In this deployment, Panorama is the server and the WildFire appliance is the client.
- Single custom certificate for a WildFire Cluster—Instead of assigning unique certificates to each WildFire appliance in a cluster, you can assign a single, shared client certificate to the entire WildFire cluster, which, in turn, allows you to push a single certificate to all WildFire appliances in the cluster instead of configuring separate certificates for each cluster member. In this scenario, Panorama is the server and the WildFire cluster is the client.
- Custom certificates for communication between Log Collectors—This allows you to configure custom server and client certificates for inter-Log Collector communication. You must configure secure server communication and secure client communication on each Log Collector in a Collector Group because the server and client roles are chosen dynamically.

The following procedure provides a high-level overview of the steps involved in deploying custom certificates on your WildFire appliance, PAN-DB appliance, or Log Collectors.

**STEP 1** Generate or obtain your server and client certificates.
Based in the needs of your organization, choose one of the supported methods for generating or obtaining your custom certificates.

**STEP 2 |** Configure the server certificate profile and SSL/TLS service profile for the server.

**STEP 3 |** Configure Secure Server Communication on the server.

**STEP 4 |** Configure the client certificate profile for the client device. The method for configuring this profile depends on your deployment.

**STEP 5 |** Configure Secure Client Communication on the client devices.

**STEP 6 |** Enforce the use of custom certificates.
GlobalProtect Features

> Optimized Split Tunneling for GlobalProtect on page 105
> Kerberos Authentication Support for macOS on page 110
> SAML SSO for GlobalProtect on Chromebooks on page 115
> OPSWAT SDK V4 Support on page 117

For more information about the features introduced in GlobalProtect app 4.1, including GlobalProtect App for Linux, see the GlobalProtect App 4.1 New Features Guide.
Optimized Split Tunneling for GlobalProtect

**Software Support:** Starting with GlobalProtect™ App 4.1 and with PAN-OS® 8.1 and later releases

**OS Support:** Windows 7 Service Pack 2 and later releases and macOS 10.10 and later releases

In addition to **route-based split tunneling**, the GlobalProtect app for Windows and macOS endpoints now supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application.

*This enhancement requires a GlobalProtect subscription.*

This enhancement enables you to:

- Tunnel enterprise SaaS and public cloud applications for comprehensive SaaS application visibility and control to avoid risks associated with Shadow IT in environments where it is not feasible to tunnel all traffic.
- Send latency-sensitive traffic, such as VoIP, outside the VPN tunnel, while all other traffic goes through the VPN for inspection and policy enforcement by the GlobalProtect gateway.
- Exclude HTTP/HTTPS video streaming traffic from the VPN tunnel. Video streaming applications, such as YouTube and Netflix, consume large amounts of bandwidth. By excluding lower risk video streaming traffic from the VPN tunnel, you can decrease bandwidth consumption on the gateway.

*The firewall App-ID functionality identifies the video stream before allowing traffic to be split tunneled.*

The following list describes the order in which the split tunnel rules are applied:
When you configure a split tunnel to include traffic based on the application process name or destination domain and port (optional), all traffic for that specific application or domain is sent through the VPN tunnel for inspection and policy enforcement. For example, you can allow all Salesforce traffic to go through the VPN tunnel using the *Salesforce.com destination domain. By including all Salesforce traffic in the VPN tunnel, you can provide secure access to the entire Salesforce domain and subdomains.

When you configure a split tunnel to exclude traffic based on the application process name or destination domain and port (optional), all traffic for that specific application or domain is sent directly to the physical adapter on the endpoint without inspection. For example, you can exclude all Skype traffic from the VPN tunnel using the C:\Program Files (x86)\Skype\Phone\Skype application process name.

Use the following steps to configure a split tunnel for public applications or video streams:

- Configure a split tunnel to include or exclude public applications based on the destination domain:
1. **Configure a GlobalProtect gateway.**
   
   Select Network > GlobalProtect > Gateways to modify an existing gateway or Add a new one.

2. Enable split tunneling.
   
   1. On the Agent > Tunnel Settings tab, enable Tunnel Mode to enable split tunneling.
   2. Configure the tunnel parameters for the GlobalProtect app.
   3. Configure a split tunnel to include or exclude SaaS or public cloud applications based on the destination domain and port (optional).

   *This feature supports both IPv4 and IPv6 traffic.*

   1. On the Agent > Client Settings tab, select an existing client setting or Add a new one.
   2. Disable the No direct access to local network option (Split Tunnel > Access Route). If enabled, this setting disables split tunneling on Windows, Linux, and macOS networks.
   3. **(Optional)** Add the SaaS or public cloud applications that you want to route to GlobalProtect through the VPN connection using the destination domain and port (Split Tunnel > Domain and Application > Include Domain). You can add up to 200 entries to the list. For example, add *.office365.com to allow all Office 365 traffic to go through the VPN tunnel.
   4. **(Optional)** Add the SaaS or public cloud applications that you want to exclude from the VPN tunnel using the destination domain and port (Split Tunnel > Domain and Application > Exclude Domain). You can add up to 200 entries to the list. For example, add *.engadget.com to exclude all Engadget traffic from the VPN tunnel.
   5. Click OK to save your client settings.

4. Save the gateway configuration.
   
   1. Click OK to save the gateway configuration.
   2. Commit your changes.

- Configure a split tunnel to include or exclude public applications based on the application process name:

   1. **Configure a GlobalProtect gateway.**
      
      Select Network > GlobalProtect > Gateways to modify an existing gateway or add a new one.

   2. Enable split tunneling.
      
      1. On the Agent > Tunnel Settings tab, enable Tunnel Mode to enable split tunneling.
      2. Configure the tunnel parameters for the GlobalProtect app.
      3. Configure a split tunnel to include or exclude SaaS or public cloud applications based on the application process name.

      *This feature supports both IPv4 and IPv6 traffic.*

   1. On the Agent > Client Settings tab, select an existing client setting or Add a new one.
   2. Disable the No direct access to local network option (Split Tunnel > Access Route). This setting disables split tunneling on Windows, Linux, and macOS networks.
   3. **(Optional)** Add the SaaS or public cloud applications that you want to route to GlobalProtect through the VPN connection using the application process name (Split Tunnel > Domain and Application > Include Client Application Process Name). You can add up to 200 entries to the list. For example, add /Application/Safari.app/Contents/MacOS/Safari to allow all Safari-based traffic to go through the VPN tunnel on macOS endpoints.
4. (Optional) Add the SaaS or public cloud applications that you want to exclude from the VPN tunnel using the application process name (Split Tunnel > Domain and Application > Exclude Client Application Process Name). You can add up to 200 entries to the list. For example, add `/Applications/Microsoft Lync.app/Contents/MacOS/MicrosoftLync` to exclude all Microsoft Lync application traffic from the VPN tunnel.

5. Click OK to save your client settings.

4. Save the gateway configuration.

1. Click OK to save the gateway configuration.
2. Commit your changes.

- Configure a split tunnel to exclude video streaming traffic:
  1. Configure a GlobalProtect gateway.
     
     Select Network > GlobalProtect > Gateways to modify an existing gateway or add a new one.

  2. Enable split tunneling.
     
     1. On the Agent > Tunnel Settings tab, enable Tunnel Mode to enable split tunneling.
     2. Configure the tunnel parameters for the GlobalProtect app.

  3. Configure a split tunnel to exclude video streaming traffic from the VPN tunnel.

     All video traffic types are redirected for the following video streaming applications:
     - YouTube
     - Dailymotion
     - Netflix

     If you exclude any other video streaming applications from the VPN tunnel, only the following video traffic types are redirected for those applications:
     - MP4
     - WebM
     - MPEG

     The App-ID functionality on the firewall identifies the video stream before traffic can be split tunneled.

     If the physical adapter on a Windows or macOS endpoint supports only IPv4 addresses, the endpoint user cannot access the video streaming applications that you exclude from the VPN tunnel when you configure the GlobalProtect gateway to assign IPv6 addresses to the virtual network adapters on the endpoints that connect to the gateway. In this case, ensure that the IP pools used to assign IP addresses to the virtual network adapters on these endpoints do not include any IPv6 addresses (Network > GlobalProtect > Gateways > Agent > Client IP Pool or Client Settings > IP Pools).

     If you exclude video streaming traffic from the VPN tunnel (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Video Traffic), do not include web browser applications, such as Firefox or Chrome, in the VPN tunnel (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Client Settings > <client-setting> > Split Tunnel > Domain and Application). This ensures that there is no conflicting logic in the split tunnel configuration and that your users can stream videos from web browsers.

     To exclude Sling TV app traffic from the VPN tunnel, use application-based split tunneling (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Client...
1. On the Agent > Video Traffic tab, enable the option to Exclude video applications from the tunnel.

   If you enable this option but do not select specific video streaming applications to exclude from the VPN tunnel, all video streaming traffic is excluded.

2. (Optional) Browse the Applications list to view all of the video streaming applications that you can exclude from the VPN tunnel. Click the add icon ( ) for the application(s) that you want to exclude. For example, click the add icon for directv to exclude DIRECTV video streaming traffic from the VPN tunnel.

3. (Optional) Add the video streaming applications that you want to exclude from the VPN tunnel using the Applications drop-down—a shortened version of the Applications list that contains some of the most popular video streaming applications. For example, select youtube-streaming from the Applications drop-down to exclude all YouTube-based video streaming traffic from the VPN tunnel.

4. Save the gateway configuration.
   1. Click OK to save the gateway configuration.
   2. Commit your changes.
Kerberos Authentication Support for macOS

Software Support: Starting with GlobalProtect™ App 4.1 and with PAN-OS® 8.0 and later releases

OS Support: macOS 10.10 and later releases

The GlobalProtect™ app for Mac endpoints now supports Kerberos V5 single sign-on (SSO) for GlobalProtect portal and gateway authentication. Kerberos SSO maintains a seamless logon experience by providing accurate User-ID™ information without user interaction. Networks that support Kerberos SSO require end users to log in only during initial network access. After the initial login, end users can access any Kerberos-enabled service in the network (such as webmail) without having to log in again until the SSO session expires (the SSO session duration is established by the Kerberos administrator). This authentication method helps identify users for user and HIP policy enforcement.

If you enable both Kerberos SSO and an external authentication service (such as RADIUS), GlobalProtect attempts SSO first. You can configure GlobalProtect to fall back to an external authentication service when SSO fails or you can configure GlobalProtect to use only Kerberos SSO for authentication.

In this implementation, the GlobalProtect portal and gateway act as Kerberos service principals and the GlobalProtect app acts as a user principal that authenticates end users with a Kerberos service ticket from the Key Distribution Center (KDC).

The following items must be in place for the GlobalProtect app for macOS endpoints to support Kerberos SSO:

- A Kerberos infrastructure, which includes a KDC with an authentication server (AS) and a ticket-granting service (TGS).

GlobalProtect supports the following KDCs:

- Microsoft Active Directory on Windows Server 2008 R2
- Microsoft Active Directory on Windows Server 2012
- MIT Kerberos V5

The KDC must be reachable from the endpoint on which the GlobalProtect app is running. In most instances, the KDC is reachable only from inside the enterprise network, which means the GlobalProtect app can use Kerberos authentication only when the endpoint is internal. However, if the KDC is reachable from outside the enterprise network (from the Internet), the GlobalProtect app can use Kerberos authentication when the endpoint is external.

If the user certificate store contains at least one certificate that is issued by the same CA as the certificate used for pre-logon tunnel establishment, you can also use Kerberos authentication with pre-logon to enable the GlobalProtect app to use Kerberos authentication when the endpoint is external.

When an end user attempts to access protected network resources using Kerberos authentication, the AS grants the user a Ticket to Get Tickets (TGT), which is a service request used to generate service tickets from the TGS. The service ticket is then used to authenticate the end user and establish a service session.

- A Kerberos service account for each GlobalProtect portal and gateway.

Service accounts are required for creating Kerberos keytabs, which are files that contain the principal name and password of each GlobalProtect portal or gateway.
- PAN-OS 8.0 or a later release.
- macOS version 10.10 or a later release.

**STEP 1** | Create a Kerberos keytab file.
1. Log in to the KDC using your Kerberos service account credentials.
2. Open a command prompt and then enter the following command:

```
ktpass /princ <principal_name> /pass <password> /crypto <algorithm> /ptype KRB5_NT_PRINCIPAL /out <file_name>.keytab
```

The `<principal_name>` and `<password>` are the principal name and password of the GlobalProtect portal or gateway. The `<algorithm>` must match the algorithm in the service ticket issued by the TGS, which is determined by the Kerberos administrator. If the GlobalProtect portal or gateway is running in FIPS or CC mode, the algorithm must be `aes128-cts-hmac-sha1-96` or `aes256-cts-hmac-sha1-96`. If the portal or gateway is not running in FIPS or CC mode, you can also use `des3-cbc-sha1` or `arcfour-hmac`.

**STEP 2** | Create a server profile for Kerberos authentication.

**STEP 3** | Import the Kerberos keytab file to an authentication profile.
1. Select **Device > Authentication Profile**.
2. Select an existing authentication profile or **Add** a new one.
3. In the **Single Sign-On** area, enter the **Kerberos Realm** (up to 127 characters), which is the domain to which the end user belongs. For example, a user with the account name `user@EXAMPLE.LOCAL` belongs to the `EXAMPLE.LOCAL` realm.
4. **Import** a **Kerberos Keytab** file to the authentication profile.

   When the Import Keytab dialog opens, **Browse** to and select the keytab file, and then click **OK**.
5. Click OK to save your changes.

STEP 4 | Assign the authentication profile to an internal gateway. If the Kerberos authentication infrastructure is deployed in an external gateway, such as a DMZ, you can also assign the authentication profile to an external gateway.

1. Select Network > GlobalProtect > Gateways to modify an existing gateway or Add a new one.

2. Select an existing SSL/TLS Service Profile for securing the gateway, or Add a new service profile (Network > GlobalProtect > Gateways > <gateway-config> > Authentication).

3. Add a Client Authentication configuration (Network > GlobalProtect > Gateways > <gateway-config> > Authentication), and then configure the following settings:
   - Name—Name of the client authentication configuration.
- **OS**—Operating systems on which the gateway can be accessed.
- **Authentication Profile**—Authentication profile to which your Kerberos keytab file was imported.
- **(Optional) Username Label**—Custom username label for GlobalProtect gateway login.
- **(Optional) Password Label**—Custom password label for GlobalProtect gateway login.
- **(Optional) Authentication Message**—Message that is displayed when end users authenticate to the gateway.

4. Click **OK** to save your changes.

**STEP 5 | Assign the authentication profile to the GlobalProtect portal.**

1. Select **Network > GlobalProtect > Portals**.
2. Select an existing portal or **Add** a new one.

3. Select an existing **SSL/TLS Service Profile** for securing the portal, or **Add** a new service profile (**Network > GlobalProtect > Portals > <portal-config> > Authentication**).

4. **Add** a **Client Authentication** configuration (**Network > GlobalProtect > Portals > <portal-config> > Authentication**), and then configure the following settings:
   - **Name**—Name of the client authentication configuration.
   - **OS**—Operating systems on which the portal can be accessed.
   - **Authentication Profile**—Authentication profile to which your Kerberos keytab file is imported.
   - **(Optional) Username Label**—Custom username label for GlobalProtect portal login.
   - **(Optional) Password Label**—Custom password label for GlobalProtect portal login.
   - **(Optional) Authentication Message**—Message that is displayed when end users log in to the portal.

5. Click **OK** to save your changes.

**STEP 6 | Configure the GlobalProtect app behavior for Kerberos authentication failure.**

1. Select **Network > GlobalProtect > Portals**.
2. Select a portal configuration.
3. Select the agent configuration that you want to modify, or **Add** a new one (**Network > GlobalProtect > Portals > <portal-config> > Agent**).
4. In the **App Configurations** area (**Network > GlobalProtect > Portals > <portal-config> > Agent > <agent-config> > App**), select one of the following options for **Use Default Authentication on Kerberos Authentication Failure**:

- **Yes**—Enables authentication to fall back so that when Kerberos authentication fails, GlobalProtect authenticates users through the default authentication method.
- **No**—GlobalProtect can use only Kerberos to authenticate users.

5. Click **OK** to save your changes.
6. Click **OK** to complete your configuration.

**STEP 7** | **Commit** the configuration.
SAML SSO for GlobalProtect on Chromebooks

**Software Support:** Starting with GlobalProtect™ App 4.1 and with PAN-OS® 8.0 and later releases

**OS Support:** Google Chrome OS 45 and later releases

The GlobalProtect app for Chromebooks (Chrome OS) now supports Security Assertion Markup Language (SAML) single sign-on (SSO). If you configure SAML as the authentication standard for Chromebooks, end users authenticate to GlobalProtect by leveraging the same login they use to access their Chromebook applications. This feature enables end users to connect to GlobalProtect automatically without having to re-enter their credentials on the GlobalProtect app.

In this implementation, Google acts as the SAML service provider while the GlobalProtect app authenticates users directly to their organization’s SAML identity provider.

*GlobalProtect currently supports only the Post SAML HTTP binding method.*

To use SAML SSO for Chrome applications, end users must install the **SAML SSO for Chrome Apps** Google extension on their Chromebooks. This extension allows users to access multiple Chrome applications during a single login session by sending the user’s SAML SSO cookies to all applications that are whitelisted by an administrator.

Use the following steps to configure SAML SSO for Chrome applications:

**STEP 1 | Set up SAML authentication for GlobalProtect.**

- Create a server profile with settings for access to the SAML authentication service.
- Create an authentication profile that refers to the SAML server profile.

**STEP 2 | Configure a GlobalProtect gateway.**

1. Specify a SAML authentication profile for Chrome gateway users.
   - On the **Authentication** tab of the GlobalProtect gateway configuration, select a SAML **Authentication Profile** or create a new SAML profile for the gateway. This profile is used to authenticate endpoints seeking access to the gateway.
2. *(Optional)* Select a **Certificate Profile** for client gateway authentication. The client certificate must be pre-deployed or deployed using the Simple Certificate Enrollment Protocol (SCEP).

**STEP 3 | Define the GlobalProtect client authentication configurations on the GlobalProtect portal.**

1. Specify a SAML authentication profile for the portal.
   - On the **Authentication** tab of the GlobalProtect portal configuration, select a SAML **Authentication Profile** or create a new SAML profile for the portal. This profile is used to authenticate endpoints seeking access to the portal.
2. *(Optional)* Select a **Certificate Profile** for client portal authentication. A valid client certificate must be pre-deployed on all Chromebooks if you configure the **Certificate Profile**.

**STEP 4 | Install the **SAML SSO for Chrome Apps** extension from Google.** This extension enables SAML SSO for Chrome applications.

Launch the Chrome **Web Store** and install the **SAML SSO for Chrome Apps** extension.

**STEP 5 | Configure SAML SSO for Chrome apps.**
• For GlobalProtect to support SAML SSO, you must add the GlobalProtect application ID (nicidmbokaedpmoegdbcebhnchpegd) to the whitelist in the SAML SSO for Chrome Apps extension configuration file.
OPSWAT SDK V4 Support

**Software Support:** Starting with GlobalProtect™ app 4.1 and with PAN-OS® 8.1 and later releases.

**OS Support:** Windows 7 and later releases and macOS 10.12 and later releases.

GlobalProtect is now integrated with OPSWAT SDK V4 to detect and assess the endpoint state and the third-party security applications running on the endpoint. OPSWAT is a security tool leveraged by the Host Information Profile (HIP) to collect information about the security status of the endpoints in the network, which is used for policy enforcement on the GlobalProtect gateway. This integration follows the end-of-life (EoL) announcement for OPSWAT SDK V3, which is the OPSWAT SDK version that GlobalProtect previously supported.

With this migration from OPSWAT SDK V3 to OPSWAT SDK V4, GlobalProtect introduces the following changes to the HIP Match log and HIP Object:

- The **Antivirus** and **Anti-Spyware** categories merged to form the new **Anti-Malware** category.
- Vendor and product names are based on OPSWAT SDK V4.
OPSWAT SDK is unable to detect the following Anti-Malware information for the Gatekeeper security feature on macOS endpoints:

- Engine Version
- Definition Version
- Date
- Last Scanned
Management Features

- Rule Usage Tracking
- Configuration Table Export
- Reporting Engine Enhancements
- Enhanced Application Logging
Rule Usage Tracking

The Panorama and firewall web interfaces now display the hit count for traffic that matches a policy rule to help keep your firewall policies up to date as your environment and security needs change over time. To prevent attackers from exploiting over-provisioned access, such as when a server is decommissioned or when you no longer require temporary access to a service, the rule usage tracking feature helps you identify and remove unused rules. Additionally, this feature provides the ability to validate rule additions and rule changes and to monitor the time frame when a rule was used. For example, when you migrate port-based rules to app-based rules, you create an app-based rule above the port-based rule and then you check for any traffic that matches the port-based rule. After migration, the hit-count data helps you determine whether it is safe to remove the port-based rule by confirming that traffic is matching the app-based rule instead of the port-based rule.

On the firewall, rule usage tracking allows you to view rule usage hit count and the last timestamp of the last hit. On Panorama, the rule usage tracking data allows you to view whether a policy rule pushed to firewalls in a specific device group has traffic matches. The rule usage tracking data gives you the information you need to determine whether a rule is effective for access enforcement. For more information, see Monitor Policy Rule Usage.

STEP 1 | Launch the firewall or Panorama web interface.

- **On a firewall**
  1. Launch the web interface and select Policies.
  2. View the rule usage statistics for each policy rule. The following information is displayed:
    - **Hit Count**—The number of times traffic matched the criteria you defined in the policy rule. Persists through reboot, dataplane restarts, and upgrades unless you manually reset or rename the rule.
    - **Last Hit**—The most recent timestamp for when traffic matched the rule.
    - **First Hit**—The first instance when traffic was matched to this rule.

- **On Panorama**
  1. Launch the web interface and select Policies.
  2. Determine whether the rule is being used (Rule Usage column). The policy rule usage status is one of the following:

    The Rule Usage column displays rule usage for each appliance in the device group. The rule usage information displayed persists through reboot, dataplane restarts, and upgrades.
- **Used**—When all appliances in the device group—to which you pushed the policy rule—have traffic matches for the policy rule.
- **Partially Used**—When some of the appliances in the device group—to which you pushed the policy rule—have matches for the policy rule.
- **Unused**—When no appliances in the device group—to which you pushed the policy rule—have traffic matches for the policy rule.

3. **Preview Rules** to view and select a specific firewall managed by Panorama to view the firewall-specific policy rule usage data. If needed, you can reset the firewall hit-count data for individual rules. Panorama retrieves rule usage information from managed firewalls every five minutes.

![Combined Rules Preview](image)

**STEP 2** | Reset the rule usage tracking count data.

You can reset the rule hit count data to validate an existing rule or to gauge rule usage within a specified period of time. Policy rule hit-count data is not stored on the firewall or Panorama so after you clear the hit count using the reset option, that data is no longer available.

1. Identify any rules you need to reset and navigate to the Hit Count column.
2. Select Reset from the drop-down. If you previously reset a rule policy hit count, you can also view the **Last Reset Time** from the drop-down.
Configuration Table Export

You can export policy rules, objects, and IPS signatures from Panorama™ and firewalls to demonstrate regulatory compliance to external auditors, to conduct periodic reviews of the firewall configuration, and to generate reports on firewall policies. This prevents you from having to give auditors direct access to Panorama or the firewall, taking screen shots, or using the XML API to generate configuration reports. From the web interface, you can export the configuration table data for policies, objects, network, firewall, and Panorama configurations, as well as the Signature exceptions in the Antivirus, Anti-Spyware, and Vulnerability Protection Security profiles, in either a PDF or CSV file.

Configuration table export works like a print function—you cannot import generated files back in to Panorama or the firewall. The data that you view on the web interface is exported to PDF/CSV and you can use these export formats to apply filters that match your report criteria and search within PDF reports to quickly find specific data. Additionally, when you export the configuration table data, a system log is generated to record the event. For more information on how to export your configurations as a PDF or CSV, see Export Configuration Table Data.
Reporting Engine Enhancements

The reporting engine has been enhanced to provide better context on network events and user activity. These enhancements give you greater visibility and control of the log data and reports you generate so that you can create intelligent policies.

<table>
<thead>
<tr>
<th>Reporting Engine Enhancements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate log directionality</td>
<td>Firewall writes logs from the perspective of who initiated the network interaction or event. For example, if you are downloading a file from a website, the threat log describes the source (SRC) of the network interaction as the individual requesting the download and describes the destination (DST) as the website from which the source is downloading the file. The client is the entity that initiates the request while the server is the entity that receives the request.</td>
</tr>
<tr>
<td>Overlay of commits and content updates in the ACC</td>
<td>User events in the ACC, such as commits and content updates, are represented as a dotted line on all time-trended line graphs. This helps you to correlate commits and upgrades with suspicious network events.</td>
</tr>
<tr>
<td>Filters for User Activity Reports</td>
<td>Use the Filter Builder to build custom filters (Monitor &gt; PDF Reports &gt; User Activity Report).</td>
</tr>
<tr>
<td>Reporting Engine Enhancements</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>On Demand Report Scheduling</td>
<td><strong>Select Run Now</strong> for a scheduled report or <strong>Pick up Later</strong> to return at a later time to retrieve the report instead of waiting for a on-demand report to generate.</td>
</tr>
</tbody>
</table>

You can also run a **Background Report** to export the generated report in your desired format (**Monitor > Manage Custom Report**). You can save only one report for pick up at a time.

<table>
<thead>
<tr>
<th>Custom reporting enhancements</th>
<th>Custom reporting is now more user friendly:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Completions are added for user, user-group, and any other items that have possible completions.</td>
</tr>
<tr>
<td></td>
<td>• Column stickiness is added between databases to keep as many columns as possible when switching between databases.</td>
</tr>
</tbody>
</table>
Enhanced Application Logging

Enhanced application logging allows the firewall to collect data specifically intended to increase visibility into network activity for the Palo Alto Networks apps and services. For example, with this extended network visibility, Magnifier—the Palo Alto Networks behavior analytics service—can better understand your normal network behavior, in order to recognize unusual behavior that might indicate attacker reconnaissance or lateral movement.

The data this feature collects is designed strictly for Palo Alto Networks apps and services to consume and process (you cannot view enhanced application logs). Only turn on this feature in consultation with your Systems Engineer (SE) and after also enabling the Palo Alto Networks logging service.

To turn on **Enable Enhanced Application Logging**, select **Device > Setup > Management > Logging Service** on the firewall web interface:

![Enable Enhanced Application Logging](image)

Then, update the log forwarding profiles that are attached to your security policy rules to **Enable enhanced application logging to Logging Service** (Objects > Log Forwarding).

![Log Forwarding Profile](image)

Notice that when you enable enhanced application logging in a Log Forwarding profile, match lists that specify the log types required for enhanced application logging are automatically added to the profile. If the Log Forwarding profile that you've updated is not yet attached to a security policy rule, be sure to add it to security policy rules to trigger log generation and forwarding for the traffic matched to those rules (select **Policies > Security > Actions > Log Forwarding** and select the Log Forwarding profile enabled with enhanced application logging).
Networking Features

> Tunnel Content Inspection Logging
> Dynamic IP Address Support for Destination NAT
> FQDN Support for IKE Gateway Peer IP Address
> Configuration Capacity Improvements
> Refresh of Default Trusted CAs
> ARP Cache Timeout
Tunnel Content Inspection Logging

To easily view tunnel inspection logs for cleartext tunnels and to separate tunnel inspection logs from traffic logs, you can now configure tunnel content inspection logging and log forwarding. You can configure tunnel content inspection to log tunnel sessions at the start of a session, the end of a session, or both. These log settings override the Security policy rule settings that would otherwise control the tunnel inspection logs. You can also override log forwarding settings in Security policy rules that control traffic logs by configuring tunnel inspection log settings to store tunnel logs separately from traffic logs. The tunnel inspection logs store the outer tunnel (GRE, non-encrypted IPSec, or GTP-U) sessions and the traffic logs store the inner traffic flows. This allows you to easily report on tunnel activity (as opposed to inner content activity) using the ACC and reporting features.

You can create a Log Forwarding profile to specify where to send tunnel inspection logs. A Log Forwarding profile for tunnel inspection is separate from a Log Forwarding profile specified in a Security policy rule, which applies to traffic logs.

When you view a detailed tunnel inspection log, the log now includes the name of the Tunnel Inspection policy rule that applied to the session captured in the log, which makes it easier to track information about non-encrypted tunnel traffic.

**STEP 1 |** Specify logging of sessions that match a tunnel inspection policy rule and configure log forwarding.
1. Select **Policies > Tunnel Inspection** and select a Tunnel Inspection policy rule.
2. Select **Inspection > Monitor Options**.
3. Select **Override Security Rule Log Setting**.
4. Select **Log at Session Start** and **Log at Session End**.
5. Select a **Log Forwarding** profile to determine where the firewall forwards tunnel logs for sessions that match the Tunnel Inspection policy rule.

**STEP 2 |** View tunnel inspection logs.
1. Select **Monitor > Logs > Tunnel Inspection**.
2. Click Detailed Log View ( ) to see details about a tunnel inspection log.
Dynamic IP Address Support for Destination NAT

**Destination NAT** is enhanced so that you can translate the original destination address to a destination host or server that has a dynamic IP address that is associated with an FQDN and can be resolved by DNS. It is especially helpful to Configure Destination NAT Using Dynamic IP Addresses in cloud deployments, which typically use dynamic IP addressing across multiple servers. Each time the host or server in the cloud receives a new (dynamic) IP address, you don’t have to manually update the NAT policy rule by continuously querying the DNS server, nor do you need to use a separate external component to update the DNS server with the latest FQDN-to-IP address mapping. The dynamic IP translation type for destination NAT is in addition to the static, one-to-one translation that continues to be supported in this and earlier releases.

If an FQDN in the translated destination NAT address resolves to more than one IP address, the firewall automatically distributes translated sessions among those addresses (based on a round-robin algorithm) to provide improved session distribution. Each FQDN can support up to 32 IPv4 addresses and 32 IPv6 addresses. If a DNS server returns more than 32 addresses for an FQDN, the firewall uses the first 32 addresses in the packet.

Using the **Dynamic IP (with session distribution)** destination address type also allows you to translate multiple original destination IP addresses to multiple translated destination IP addresses. A many-to-many translation means, for example, that three original destination IP addresses and four translated destination IP addresses can result in 12 possible destination NAT translations using a single NAT rule.

*You can configure the frequency at which the firewall refreshes an FQDN (Use Case 1: Firewall Requires DNS Resolution for Management Purposes).*

**STEP 1** | Create an address object using the FQDN of the ELB or server to which you want to translate the address.

**STEP 2** | Create the destination NAT policy.

1. Specify the original packet to use the publicly routed IP address of the service hosted behind the firewall.
2. Configure the **Translation Type** for the translated packet as **Dynamic IP (with session distribution)**.
3. Enter the FQDN address object (that you created) as the **Translated Address**.
4. Click **OK**.

**STEP 3 | Commit your changes.**
FQDN Support for IKE Gateway Peer IP Address

When you configure an IPSec tunnel with an IKE gateway peer, you can now configure that address as an FQDN or an address object that uses an FQDN. Using an FQDN for the peer address saves you from repeatedly reconfiguring peer addresses in several scenarios. An FQDN prevents IKE exchange problems that arise when many branch offices use a DHCP-assigned address on their external interface and that dynamic address changes. Similarly, FQDNs are a benefit in cloud environments where AWS and Azure use dynamic addresses as IKE termination points.

Another use case is when you have several satellite offices with multiple hub locations and VPN connectivity between firewalls at the satellites and hub gateway. You can configure each satellite office to use an FQDN for the IKE peer address object, so that if one hub goes down, the DNS server for that FQDN then resolves the FQDN to the IP address for the second hub. You don’t have to reconfigure the IKE peer to use the IP address of the second hub.

**STEP 1 | Set up an IKE gateway.**
Perform the first two steps to Set Up an IKE Gateway (define the gateway and establish the local endpoint of the tunnel).

**STEP 2 | Specify the IKE peer IP address for the peer at the far end of the tunnel (gateway) as an FQDN.**
You can enter the FQDN string directly or use the FQDN in an address object.

**STEP 3 | Continue to Set Up an IKE Gateway, resuming with the step where you specify how the peer is authenticated.**
Configuration Capacity Improvements

Various firewall models support larger configuration capacities in PAN-OS® 8.1 than in earlier PAN-OS releases. These increases ease your migration to Palo Alto Networks® firewalls and your deployment growth. The increased capacities are:

<table>
<thead>
<tr>
<th>Capacity Description</th>
<th>All Firewall Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Characters per Rule Name</td>
<td>63</td>
</tr>
</tbody>
</table>

PA-220 firewalls support more Security policy rules:

<table>
<thead>
<tr>
<th>Capacity Description</th>
<th>PA-220</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Policy</td>
<td>500</td>
</tr>
</tbody>
</table>

PA-3000 Series firewalls support the following capacities:

<table>
<thead>
<tr>
<th>Capacity Description</th>
<th>PA-3020</th>
<th>PA-3050</th>
<th>PA-3060</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Groups</td>
<td>750</td>
<td>1,500</td>
<td>1,500</td>
</tr>
<tr>
<td>Service Groups</td>
<td>375</td>
<td>375</td>
<td>375</td>
</tr>
<tr>
<td>Service Entries per Service Group</td>
<td>1,000</td>
<td>1,000</td>
<td>1,000</td>
</tr>
<tr>
<td>Zones</td>
<td>40</td>
<td>40</td>
<td>60</td>
</tr>
</tbody>
</table>

PA-5220 firewalls support the following increased capacities:

<table>
<thead>
<tr>
<th>Capacity Description</th>
<th>PA-5220</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Relay Agents</td>
<td>2,048</td>
</tr>
<tr>
<td>(On the PA-5220 firewall, you can a maximum of 500 DHCP servers; the maximum number of DHCP relay agents is 2,048 minus the number of configured DHCP servers.)</td>
<td></td>
</tr>
<tr>
<td>FQDN Address Objects</td>
<td>6,144</td>
</tr>
<tr>
<td>Zones</td>
<td>2,500</td>
</tr>
</tbody>
</table>

PA-5250, PA-5260, and PA-7000 Series firewalls support the following increased capacities:

<table>
<thead>
<tr>
<th>Capacity Description</th>
<th>PA-5250 and PA-5260</th>
<th>PA-7000 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Objects</td>
<td>160,000</td>
<td>160,000</td>
</tr>
<tr>
<td>Capacity Description</td>
<td>PA-5250 and PA-5260</td>
<td>PA-7000 Series</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Address Groups</td>
<td>80,000</td>
<td>80,000</td>
</tr>
<tr>
<td>Service Objects</td>
<td>12,000</td>
<td>12,000</td>
</tr>
<tr>
<td>Service Groups</td>
<td>6,000</td>
<td>6,000</td>
</tr>
<tr>
<td>Service Entries per Service Group</td>
<td>2,500</td>
<td>2,500</td>
</tr>
<tr>
<td>FQDN Address Objects</td>
<td>6,144</td>
<td>6,144</td>
</tr>
<tr>
<td>Zones</td>
<td>17,000</td>
<td>4,000</td>
</tr>
<tr>
<td>Security Policy</td>
<td>65,000</td>
<td>65,000</td>
</tr>
<tr>
<td>Tunnel Inspection Policy</td>
<td>8,500</td>
<td>8,500</td>
</tr>
<tr>
<td>DHCP Relay Agents</td>
<td>4,096*</td>
<td>4,096*</td>
</tr>
</tbody>
</table>

* On these models, you can have a maximum of 500 DHCP servers; the maximum number of DHCP relay agents is 4,096 minus the number of configured DHCP servers.

PA-820 and PA-850 firewalls support the following increased capacities:

<table>
<thead>
<tr>
<th>Capacity Description</th>
<th>PA-820</th>
<th>PA-850</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum SSL Inbound Certificates</td>
<td>75</td>
<td>100</td>
</tr>
<tr>
<td>SSL Certificate Cache Entries</td>
<td>1,000</td>
<td>2,000</td>
</tr>
</tbody>
</table>
Refresh of Default Trusted CAs

The certificate authorities (CAs) that the firewall trusts by default are updated in PAN-OS 8.1; new trusted root CAs are added and expired CAs are removed. The pre-installed list of CAs includes the most common and trusted certificate providers responsible for issuing the certificates the firewall requires to secure connections to the internet. Because the firewall trusts these CAs by default, the only additional CAs you might want to add are any trusted enterprise CAs that your organization requires.

To view and manage the list of CAs that the firewall trusts by default, select Device > Certificate Management > Certificates > Default Trusted Certificate Authorities. For details on the different keys and certificates that the firewall uses, and how to obtain and manage them, see Certificate Management.
ARP Cache Timeout

You can change the length of time that the firewall keeps IP address-to-hardware address mappings in its ARP cache to suit your environment.

**STEP 1** Access the CLI and specify how many seconds the firewall keeps ARP entries in its cache. Use the operational CLI command `set system setting arp-cache-timeout <value>`; range is 60 to 65,535, default is 1,800.

**STEP 2** View the ARP cache timeout setting with the operational CLI command `show system setting arp-cache-timeout`. 
User-ID Features

> Support for Multiple Username Formats
Support for Multiple Username Formats

The firewall can now identify a user even if different User-ID sources send usernames in different formats. For example, a single user may have multiple usernames that are represented in different formats (jane.doe@domain.com, DOMAIN\jdoe, jdoe)

The usernames are matched based on the user attributes that the firewall reads from the LDAP-compliant directory. You can specify which user attributes to collect from the directory using the Group Mapping profile.

Because the firewall now supports multiple user attributes, you should specify an attribute as the Primary Username for users. The primary username represents the user in the logs, reports, and in the policy configuration.

If your User-ID sources send usernames without an associated domain and your usernames are unique, you can also configure the firewall to not consider the domain when matching users. If you enable this option and the firewall finds more than one matching username, an error displays to indicate the username is not unique.

For more information, refer to the PAN-OS 8.1 Admin Guide.

**STEP 1** | Select Device > Server Profiles > LDAP and Add an LDAP server profile.

**STEP 2** | Select Device > User Identification > Group Mapping and configure Group Mapping using the LDAP server profile you added in the previous step.

**STEP 3** | Specify the Primary Username attribute that will identify users and optionally specify additional attributes for users or groups, then Commit your changes.

> If the Primary Username is in User Principal Name (UPN) format, it will not be normalized in the domain\username format as in previous versions. For example, if the Primary Username is received in the UPN format, it will be displayed as username@domain, not domain\username.

- For users:
  1. Select Device > User Identification > Group Mapping > Add > User and Group Attributes and specify a Primary Username (for example, userPrincipalName or sAMAccountName).
  2. (Optional) Specify additional alternate attributes to identify users. Specify User Attributes, such as an E-Mail or up to three Alternate Usernames.

- For groups:
  2. Specify Group Attributes such as the Group Name, Group Member, or E-Mail.
STEP 4 | Use the groups or usernames collected from the group mapping profile to Enable User- and Group-Based Policy:

1. (Optional) Select Device > User Identification > User-ID Agent Setup > Cache and Edit to Allow matching usernames without domain, which allows the firewall to match users if the domain is not provided. This option is disabled by default.

   If you select this option, only users retrieved during group mapping can be matched.

STEP 5 | Map users based on information from User-ID sources by configuring User-ID to gather IP-user mappings from sources using the Integrated User-ID Agent or the Windows User-ID Agent.

STEP 6 | Verify the user mapping is successful:

- To verify the Group Mapping configuration, select the Group Include List to confirm the firewall has fetched all of the groups.
- To verify all the user attributes have been captured correctly, use the `show user user-attributes user all` command.
- Verify the usernames are displayed correctly in the Source User column of the Monitor tab.
• Select Monitor > Logs > User-ID and check the User Provided by Source column to verify the users are mapped to the correct username.
WildFire Features

> WildFire Appliance-to-Appliance Encryption on page 145

For more information about the features introduced in the WildFire cloud, see the WildFire What’s New Guide.
WildFire Appliance-to-Appliance Encryption

You can now encrypt WildFire® communications between appliances deployed in a cluster. Prior to 8.1 and by default, WildFire appliances send data using cleartext when communicating with management appliances as well as WildFire cluster peers. You can use either predefined or custom certificates to authenticate connections between WildFire appliance peers using the IKE/IPsec protocol. The predefined certificates meet current FIPS/CC/UACPL-approved certification and compliance requirements. If you want to use custom certificates instead, you must select a FIPS/CC/UACPL-compliant certificate or you will not be able to import the certificate.

You can configure WildFire appliance-to-appliance encryption locally using the WildFire CLI or centrally through Panorama. Keep in mind, all WildFire appliances within a given cluster must run a version of PAN-OS that supports encrypted communications.

*If the WildFire appliances in your cluster uses FIPS/CC mode, encryption is automatically enabled using predefined certificates.*

Before configuring WildFire appliance-to-appliance encryption, be sure to review your existing WildFire secure communications configuration. If you previously configured the WildFire appliance and the firewall for secure communications using a custom certificate, you can use that custom certificate and the requisite DNS name for configuring secure communications between WildFire appliances.

*It is imperative that you use the correct, matching DNS name in the register firewall to: field in Panorama. Failure to do so will prevent appliance-to-appliance encryption from working as intended.*

The following tables describe the high-level tasks involved in configuring WildFire appliance-to-appliance encryption. For detailed instructions on these tasks, refer to the WildFire Administration Guide for the full installation procedure.

**Table 2: WildFire Appliance-to-Appliance Encryption Installation Tasks Using Panorama**

<table>
<thead>
<tr>
<th>Configuration Using Custom Certificates through Panorama</th>
<th>Configuration Using Predefined Certificates through Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. In the <strong>Panorama &gt; Managed WildFire Clusters &gt; WildFire Cluster</strong> page:</td>
<td>1. In the <strong>Panorama &gt; Managed WildFire Clusters &gt; WildFire Cluster</strong> page:</td>
</tr>
<tr>
<td>• Configure the DNS name used for authentication found in the custom certificate.</td>
<td>• Enable Secure Cluster Communication.</td>
</tr>
<tr>
<td>• Enable customize secure server communication and configure the SSL/TLS Service Profile and certificate profile to define the custom certificate for encrypted communication between WildFire peers.</td>
<td>• Enable HA Traffic Encryption.</td>
</tr>
<tr>
<td>• Import or generate a custom certificate. If you are generating a custom certificate, be sure to use the same DNS stated in the certificate.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3: WildFire Appliance-to-Appliance Encryption Installation Tasks Using the CLI

<table>
<thead>
<tr>
<th>Configuration Using Custom Certificates through the WildFire CLI</th>
<th>Configuration Using Predefined Certificates through the CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To configure the WildFire appliance for encrypted communications</strong>, you must enable and configure the following on the active-controller in 2-node clusters. If your cluster has 3 or more nodes, you must also duplicate the configuration on the server nodes.</td>
<td></td>
</tr>
</tbody>
</table>

1. **In the Panorama > Managed WildFire Clusters > WildFire Cluster page:**
   - Configure the DNS name used for authentication found in the custom certificate.
   - Enable customize secure server communication and configure the SSL/TLS Service Profile and certificate profile to define the custom certificate for encrypted communication between WildFire peers.
   - Import or generate a custom certificate. If you are generating a custom certificate, be sure to use the same DNS stated in the certificate.

2. Configure the firewall secure communication settings to use the custom certificate. This enables the WildFire cluster to communicate with the firewall using encryption.

3. From the WildFire appliance cluster active-controller CLI:
   - Enable secure cluster communication.
   - Enable HA traffic encryption.
<table>
<thead>
<tr>
<th>Configuration Using Custom Certificates through the WildFire CLI</th>
<th>Configuration Using Predefined Certificates through the CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enable HA traffic encryption.</td>
<td></td>
</tr>
</tbody>
</table>