



# PAN-OS® 8.0 Release Notes

## Release 8.0.2

Revision Date: May 5, 2017

Review important information about Palo Alto Networks PAN-OS 8.0 software, including new features introduced, workarounds for open issues, and issues that are addressed in the PAN-OS 8.0 release. For installation, upgrade, and downgrade instructions, refer to the [PAN-OS 8.0 New Features Guide](#). For the latest version of these release notes, refer to the Palo Alto Networks [technical documentation portal](#).



HSM storage of the master key on firewalls running PAN-OS 8.0.0 or PAN-OS 8.0.1 is not supported. See the [PAN-75960](#) known issue description for details.

- PAN-OS 8.0 Release Information ..... 3**
- Features Introduced in PAN-OS 8.0 ..... 4
  - Management Features ..... 5
  - Panorama Features ..... 6
  - Content Inspection Features ..... 8
  - WildFire Features ..... 10
  - Authentication Features ..... 11
  - User-ID Features ..... 12
  - App-ID Features ..... 13
  - Decryption Features ..... 13
  - Virtualization Features ..... 14
  - Networking Features ..... 16
  - GlobalProtect Features ..... 18
- Changes to Default Behavior ..... 20
  - Authentication Changes ..... 20
  - Content Inspection Changes ..... 20
  - GlobalProtect Changes ..... 22
  - Management Changes ..... 22
  - Panorama Changes ..... 23
  - VM-Series Firewall Changes ..... 24
  - WildFire Changes ..... 24
- CLI and XML API Changes in PAN-OS 8.0 ..... 26
  - Authentication CLI Changes ..... 26
  - Content Inspection CLI Changes ..... 27
  - GlobalProtect CLI Changes ..... 28
  - Management CLI Changes ..... 28
  - User-ID CLI Changes ..... 29

Associated Software and Content Versions .....	30
Limitations.....	31
Known Issues .....	32
Known Issues Related to PAN-OS 8.0 Releases .....	32
Known Issues Specific to the WF-500 Appliance.....	48
<b>PAN-OS 8.0.2 Addressed Issues .....</b>	<b>53</b>
<b>PAN-OS 8.0.1 Addressed Issues .....</b>	<b>59</b>
<b>PAN-OS 8.0.0 Addressed Issues .....</b>	<b>63</b>
<b>Getting Help.....</b>	<b>71</b>
Related Documentation.....	71
Requesting Support .....	72

# PAN-OS 8.0 Release Information

---

- ▲ [Features Introduced in PAN-OS 8.0](#)
- ▲ [Changes to Default Behavior](#)
- ▲ [CLI and XML API Changes in PAN-OS 8.0](#)
- ▲ [Associated Software and Content Versions](#)
- ▲ [Limitations](#)
- ▲ [Known Issues](#)



HSM storage of the master key on firewalls running PAN-OS 8.0.0 or PAN-OS 8.0.1 is not supported. See the [PAN-75960](#) known issue description for details.



Previously known issues carried over from previous release notes and that were identified using legacy ID numbers (5 or 6 digits without a prefix) are now assigned new issue ID numbers that also include product-specific prefixes.

- ▲ [PAN-OS 8.0.2 Addressed Issues](#)
- ▲ [PAN-OS 8.0.1 Addressed Issues](#)
- ▲ [PAN-OS 8.0.0 Addressed Issues](#)
- ▲ [Getting Help](#)

## Features Introduced in PAN-OS 8.0

The following topics describe the new features introduced in the PAN-OS® 8.0 release, which requires content release version 655 or a later version. For [upgrade and downgrade considerations](#) and for specific information about [the upgrade path for a firewall](#), refer to the [Upgrade](#) section of the [PAN-OS 8.0 New Features Guide](#). The new features guide also provides additional information about how to use the new features in this release.

- ▲ [Management Features](#)
- ▲ [Panorama Features](#)
- ▲ [Content Inspection Features](#)
- ▲ [WildFire Features](#)
- ▲ [Authentication Features](#)
- ▲ [User-ID Features](#)
- ▲ [App-ID Features](#)
- ▲ [Decryption Features](#)
- ▲ [Virtualization Features](#)
- ▲ [Networking Features](#)
- ▲ [GlobalProtect Features](#)

## Management Features

New Management Features	Description
Administrator-Level Commit and Revert	You can now <a href="#">commit, validate, preview, save, and revert changes</a> that you made in a Panorama or firewall configuration independent of changes that other administrators have made. This simplifies your configuration workflow because you don't have to coordinate commits with other administrators when your changes are unrelated to theirs, or worry about reverting changes other administrators made that weren't ready.
NetFlow Support for PA-7000 Series Firewalls	PA-7000 Series firewalls now have the same ability as other Palo Alto Networks firewalls to <a href="#">export NetFlow records</a> for IP traffic flows to a NetFlow collector. This gives you more comprehensive visibility into how users and devices are using network resources.
PA-7000 Series Firewall Log Forwarding to Panorama	You can now <a href="#">forward logs from PA-7000 Series firewalls</a> to Panorama for improved log retention, which helps you meet regulatory requirements for your industry as well as your internal log archival requirements.
Selective Log Forwarding Based on Log Attributes	To enable your organization to process and respond to incident alerts more quickly, you can now <a href="#">create custom log forwarding filters</a> based on any log attributes. Instead of forwarding logs based only on severity levels, you can forward just the information that various teams in your organization want to monitor or act on. For example, a security operations analyst who investigates malware incidents might be interested only in Threat logs with the type attribute set to wildfire-virus.
Action-Oriented Log Forwarding using HTTP	<p>The firewall can now directly forward logs using HTTP/HTTPS so that you can trigger an automated action when a specific event occurs. This capability allows the firewall to integrate with external systems that provide an HTTP-based API. And, combined with the <a href="#">Selective Log Forwarding Based on Log Attributes</a>, you can now automate security workflow more efficiently, applying dynamic policy, and responding to security incidents.</p> <ul style="list-style-type: none"> <li>• Trigger an action or a workflow on a third-party service that provides an HTTP-based API: The firewall can now send an HTTP request as an API call. You can select the HTTP method, and customize the header, request format, and payload to trigger an action. For example, on an HA failover event, the firewall can generate an HTTP request to an IT management service to automatically create an incident report with the details in the system log. This automated workflow can help the IT infrastructure team to easily track and follow up on the issue.</li> <li>• Enable dynamic policy and enforcement: Tag the source or destination IP address in a log entry, register the tags to connected User-ID agents, and take action to enforce policy at every location on your network. For example, when a Threat log indicates that the firewall has detected malware, you can tag the source or destination IP address to quarantine the malware-infected device. Based on the tag, the IP address associated with the device becomes the member of a dynamic address group, and the Security policy rule in which the dynamic address group is referenced limits access to corporate resources until IT clears the device for use.</li> </ul>

New Management Features (Continued)	Description
Extended SNMP Support	<p>PAN-OS support for Simple Network Management Protocol (<a href="#">SNMP</a>) now includes the following features:</p> <ul style="list-style-type: none"> <li>• Logging statistics—Using SNMP to monitor logging statistics for firewalls and Log Collectors helps you plan improvements to your log collection architecture, evaluate the health of firewall and Panorama logging functions, and troubleshoot issues such as dropped logs. You can now monitor a broader range of logging statistics, including log rate, disk usage, retention periods, the forwarding status from individual firewalls to Panorama and external servers, and the status of firewall-to-Log Collector connections.</li> <li>• HA2 statistics and traps—Monitoring SNMP statistics and traps for the interfaces that firewalls use for high availability (HA) synchronization helps you troubleshoot and verify the health of HA functions such as state changes. You can now use an SNMP manager to monitor the dedicated HA2 interfaces of firewalls, in addition to the HA1, HA2 backup, and HA3 interfaces.</li> </ul>
Increased Storage on PA-7000 Series Firewall	<p>To provide longer retention periods for logs on the PA-7000 Series firewall, you can now <a href="#">increase the log storage capacity</a> to 4TB by installing 2TB disks in the two RAID disk pairs (formerly only 1TB disks were supported). For log storage beyond 4TB, you can enable <a href="#">PA-7000 Series Firewall Log Forwarding to Panorama</a>, which supports up to 24TB for each M-500 appliance in the Collector Group.</p>

## Panorama Features

New Panorama Features	Description
Log Query Acceleration	<p>Panorama has an improved log query and reporting engine to enable a significant improvement in speed when generating reports and executing queries. All logs generated after the upgrade to PAN-OS 8.0 automatically take advantage of the improved query processing architecture. To extend the performance improvements for older logs, you can migrate the logs to the new format.</p>
Logging Enhancements on the Panorama Virtual Appliance	<p>You can now <a href="#">create a Log Collector</a> that runs locally on the Panorama virtual appliance. Because the local Log Collector supports multiple virtual logging disks, you can increase log storage as needed while preserving existing logs. You can increase log storage to a maximum of 24TB for a single Panorama and up to 48TB for a high availability pair. Using a local Log Collector also enables faster report generation (see <a href="#">Log Query Acceleration</a>).</p>
Increased Log Storage Capacity	<p>To provide adequate disk space for a longer log retention period, you can increase the log storage capacity on the <a href="#">M-500 appliance</a> and <a href="#">Panorama virtual appliance</a> to 24TB (formerly 8TB). The M-500 appliance now supports 2TB disks and up to 12 RAID disk pairs (formerly 1TB * 8 RAID disk pairs). In addition, the Panorama virtual appliance now supports a local Log Collector with up to 24TB of virtual disk space (see <a href="#">Logging Enhancements on the Panorama Virtual Appliance</a>).</p>

New Panorama Features	Description
Traps Logs on Panorama	<p>Panorama can now ingest Traps logs sent by the Traps Endpoint Security Manager using syslog over UDP, TCP, or SSL so that you can monitor security events relating to protected processes and executable files on Traps protected endpoints. You can filter on any log attribute and answer day-to-day operational questions such as, "How many different prevention events did a specific user trigger?"</p> <p>The ability to see Traps logs in the same context as the firewall logs allows you to correlate discrete activity observed on the network and the endpoints. Correlated events help you see the overall picture across your network and the endpoints so that you can detect any risks that evade detection or take advantage of blind spots, and strengthen your security posture well before any damage occurs.</p>
Extensible Plug-in Architecture	<p>Panorama now supports a plug-in architecture to enable new third-party integrations or updates to existing integrations (such as the VMware NSX integration) outside of a new PAN-OS feature release. Panorama displays only the interface elements pertinent to the plug-ins you install.</p> <p>The first implementation of this architecture enables <a href="#">VM-Series NSX Integration Configuration through Panorama</a>.</p>
Extended Support for Multiple Panorama Interfaces	<p>To support the demands for network segmentation and security in large-scale deployments, you can now <a href="#">separate the management functions</a> from the device management and log collection functions on the Panorama M-Series appliances. The key improvements are:</p> <ul style="list-style-type: none"> <li>• Forward logs from the managed firewalls to Panorama and the Log Collectors on multiple interfaces, instead of a single interface. This change reduces the traffic load on an interface and provides flexibility in logging to a common infrastructure across different subnets without requiring changes to the network configuration and access control lists in your infrastructure.</li> <li>• Manage the configuration for firewalls and log collectors using multiple interfaces on Panorama. This capability simplifies the management of devices that belong to different subnets or are segmented for better security.</li> <li>• Deploy software and content updates to managed firewalls and log collectors using an interface of your choice. You can continue to use the management port or select a different interface for deploying updates to managed firewalls and log collectors running PAN-OS 8.0. See <a href="#">Streamlined Deployment of Software and Content Updates from Panorama</a>.</li> </ul> <p>The ability to separate these functions across multiple interfaces reduces the traffic on the dedicated management (MGT) port. You can now lock down the management port for administrative access to Panorama (HTTPS and SSH) and the Log Collectors (SSH) only; by default Collector Group communication is enabled on the management port but you can assign a different port for this traffic.</p>
Device Group, Template, and Template Stack Capacity Increase	<p>Panorama now supports up to 1,024 <a href="#">device groups</a> and 1,024 <a href="#">templates</a> (previously 512 each), and 1,024 <a href="#">template stacks</a> (previously 128). In large-scale deployments, these capacity improvements increase administrative ease in centrally managing from Panorama and reduce the configuration exceptions and overrides that you must manage locally on individual firewalls.</p>
Streamlined Deployment of Software and Content Updates from Panorama	<p>You can now <a href="#">deploy software and content updates</a> to managed devices more quickly. Instead of pushing the updates to one device at a time, Panorama now notifies firewalls and Log Collectors when updates are available and the devices then retrieve the updates in parallel.</p> <p>The <a href="#">Extended Support for Multiple Panorama Interfaces</a> enables you to configure a separate interface, instead of using the management (MGT) interface, for deploying content and software updates to managed devices.</p>

## Content Inspection Features

New Content Inspection Features	Description
Credential Phishing Prevention	Phishing sites are sites that attackers disguise as legitimate websites with the aim to steal user information, especially the passwords that provide access to your network. You can now identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site's URL category. This feature integrates with User-ID (group mapping or user mapping, depending on which method you choose to detect credentials) to enable the firewall to detect when users are attempting to submit their corporate username and or username and password and block the submission.
Telemetry	<p>You can now participate in a community-driven approach to threat prevention through telemetry. Telemetry allows your firewall to periodically collect and share information about applications, threats, and device health with Palo Alto Networks. Palo Alto Networks uses the threat intelligence collected from you and other customers to improve the quality of intrusion prevention system (IPS) and spyware signatures and the classification of URLs in PAN-DB. For example, when a threat event triggers vulnerability or spyware signatures, the firewall shares the URLs associated with the threat with the Palo Alto Networks threat research team, so they can properly classify the URLs as malicious. Telemetry also allows Palo Alto Networks to rapidly test and evaluate experimental threat signatures with no impact to your network, so that critical threat prevention signatures can be released to all customers faster.</p> <p>You have full control over which data the firewall shares through telemetry, and samples of this data are available to view through your Telemetry settings. Palo Alto Networks does not share your telemetry data with other customers or third-party organizations.</p>
Palo Alto Networks Malicious IP Address Feeds	Palo Alto Networks now provides malicious IP address feeds that you can use to help secure your network from known malicious hosts on the Internet. One feed contains IP addresses verified as malicious by Palo Alto Networks, and another feed contains malicious IP addresses from reputable third-party threat advisories. Palo Alto Networks maintains both feeds, which you can reference in Security policy rules to allow or block traffic. You can also create your own external dynamic lists based on these feeds and customize them as needed. You must have an active Threat Prevention license to view and use the Palo Alto Networks malicious IP address feeds.
Enhanced Coverage for Command-and-Control (C2) Traffic	C2 signatures—signatures that detect where a compromised system is surreptitiously communicating with an attacker's remote server—are now generated automatically. While C2 protection is not new, previous signatures looked for an exact match to a domain name or a URL to identify a C2 host. The new, automatically-generated C2 signatures detect certain patterns in C2 traffic, providing more accurate, timely, and robust C2 detection even when the C2 host is unknown or changes rapidly.
Data Filtering Support for Data Loss Prevention (DLP) Solutions	Data filtering is enhanced to work with third-party, endpoint DLP solutions that populate file properties to indicate sensitive content, enabling the firewall to enforce your DLP policy. To better secure this confidential data, you can now create Data Filtering profiles that identify the file properties and values set by a DLP solution and then log or block the files the Data Filtering profile identifies.



New Content Inspection Features (Continued)	Description
External Dynamic List Enhancements	<p>New enhancements provide better security, flexibility, and ease-of-use when working with external dynamic lists. The enhancements include the options to:</p> <ul style="list-style-type: none"> <li>• Enable <a href="#">Authentication for External Dynamic Lists</a> to validate the identity of a list source and to forward login credentials for access to external dynamic lists that enforce basic HTTP authentication.</li> <li>• Use new <a href="#">Palo Alto Networks Malicious IP Address Feeds</a> in security policy rules to block traffic from malicious IP addresses.</li> <li>• View the contents of an external dynamic list directly on the firewall, with the option to exclude entries or view threat intelligence associated with an entry in AutoFocus.</li> </ul>
New Scheduling Options for Application and Threat Content Updates	<p>The firewall can now check for the latest App-ID, vulnerability protection, and anti-spyware signatures every 30 minutes or hourly, in addition to being able to check for these updates daily and weekly. This feature enables more immediate coverage for newly-discovered threats and strengthens safe enablement for updated and newly-defined applications.</p>
Five-Minute Updates for PAN-DB Malware and Phishing URL Categories	<p>The Malware and Phishing URL categories in PAN-DB are now updated every five minutes, based on the latest malicious and phishing sites WildFire identifies. These more frequent updates ensure that the firewall is equipped with the very latest information to detect and then block access to malicious and phishing sites.</p>
Globally Unique Threat IDs	<p>All Palo Alto Networks threat signatures now have permanent, globally unique IDs that you can use to look up threat signature information and create permanent threat exceptions:</p> <ul style="list-style-type: none"> <li>• Change the action (for example, block or alert) the firewall uses to enforce a threat signature—threat exceptions are useful if a signature is triggering false positives.</li> <li>• Easily check if a threat signature is configured as an exception.</li> <li>• Use threat IDs in the Threat Vault and AutoFocus to gain context for a threat signature.</li> </ul>
New Predefined File Blocking Profiles	<p>Two new predefined File Blocking profiles—basic file blocking and strict file blocking—have been added via content release version 653. You can use these profiles to quickly and easily apply the best practice file blocking settings to your Security policy allow rules to ensure that users are not inadvertently downloading malicious content into your network or exfiltrating sensitive data out of your network in legitimate application traffic.</p>

## WildFire Features



The PAN-OS 8.0.0 release is not available for WF-500 appliances.

New WildFire Features	Description
WildFire Appliance Clusters	In environments where you cannot use the WildFire public cloud, you can now configure up to twenty WF-500 appliances in a cluster on a single network. Creating <a href="#">WildFire appliance clusters</a> helps you scale analytical and storage capabilities to support a much larger network of firewalls, increases reliability by allowing you to configure high availability (HA) to provide fault tolerance, and provides single signature package distribution for all connected firewalls based on the activity in your cluster. You can manage WildFire clusters and standalone WF-500 appliances from Panorama.
Preferred Analysis for Documents or Executables	You can now choose to <a href="#">dedicate WildFire appliance analysis resources to either documents or executables</a> . If you are using the WildFire appliance to analyze specific file types (for example, Word documents and PDFs), this allows you to utilize all analysis resources for those file types. Previously, analysis environments were statically allocated and the resources available for document and executable analysis were evenly divided.
Verdict Changes	You can now modify the verdict that the WildFire appliance applies to a sample. <a href="#">Verdict changes</a> are applied only to locally-analyzed samples.
Verdict Checks with the WildFire Global Cloud	The <a href="#">WildFire appliance can now look up sample verdicts in the WildFire global cloud</a> before locally-analyzing the sample. The WildFire appliance can then deliver a quick verdict for samples known to the WildFire global cloud, and direct analysis resources toward files that are truly unknown to both your private network and the WildFire global community.
WildFire Analysis of Blocked Files	The new <a href="#">WildFire Analysis of Blocked Files</a> enables the firewall to submit blocked files that match existing antivirus signatures for WildFire analysis, in addition to unknown files, so that WildFire can extract valuable information from new malware variants. Malware signatures often match multiple variants of the same malware family, and as such, block new malware variants that the firewall has never seen before. Sending these blocked malware samples for WildFire analysis allows WildFire to analyze them for additional URLs, domain names, and IP addresses that must be blocked. Since all WildFire analysis data is also available on AutoFocus, you can now use WildFire and AutoFocus together to get a more complete perspective of all threats targeting your network, improving the efficacy of your security operations, incident response, and threat intelligence functions.
WildFire Phishing Verdict	The new <a href="#">WildFire Phishing Verdict</a> classifies phishing links detected in emails separately from other emailed links found to be exploits or malware. The firewall logs WildFire submissions that are phishing links to indicate that such a link has been detected in an email.  With both a WildFire license and a PAN-DB license, you can block access to phishing sites within 5 minutes of initial discovery.  The WF-500 appliance does not support the new phishing verdict, and continues to classify suspected phishing sites as malicious.

## Authentication Features

New Authentication Features	Description
SAML 2.0 Authentication	<p>The firewall and Panorama can now function as Security Assertion Markup Language (SAML) 2.0 service providers to <a href="#">enable single sign-on and single logout</a> for end users (see <a href="#">SAML 2.0 Authentication for GlobalProtect</a>) and for administrators. SAML enhances the user experience by enabling a single, interactive login to provide automatic access to multiple authenticated services that are internal or external to your organization.</p> <p>In addition to authenticating administrator accounts that are local to the firewall and Panorama, you can use SAML to authenticate and assign roles to external administrator accounts in the identity provider (IdP) identity store.</p>
Authentication Policy and Multi-Factor Authentication	<p>To protect your network resources from attackers, you can use the new <a href="#">Authentication policy</a> to ensure all your end users authenticate when they access those resources. Authentication policy is an improved replacement for Captive Portal policy, which enforced authentication only for some users. Authentication policy has the additional benefit of enabling you to choose how many authentication challenges of different types (factors) users must respond to. Using multiple factors of authentication (MFA) is particularly useful for protecting your most sensitive resources. For example, you can force users to enter a login password and then enter a verification code that they receive by phone. This approach ensures attackers can't invade your network and move laterally through it just by stealing passwords. If you want to spare users the hassle of responding to multiple challenges for resources that don't need such a high degree of protection, you can also have Authentication policy rules that enforce only password or certificate authentication.</p> <p>The firewall makes it easy to implement MFA in your network by integrating directly with several MFA platforms (Duo v2, Okta Adaptive, and PingID) and integrating through RADIUS with all other MFA platforms.</p>
TACACS+ User Account Management	<p>To use a Terminal Access Controller Access-Control System Plus (TACACS+) server for centrally managing all administrative accounts, you can now <a href="#">use Vendor-Specific Attributes (VSAs)</a> to manage the accounts of firewall and Panorama administrators. TACACS+ VSAs enable you to quickly reassign administrator roles and access domains without reconfiguring settings on the firewall and Panorama.</p>
Authentication Using Custom Certificates	<p>You can now <a href="#">deploy custom certificates</a> to replace the predefined certificates shipped on Palo Alto Networks devices for management connections between Panorama, firewalls, and Log Collectors. By generating and deploying unique certificates for each device, you can establish a unique chain of trust between Panorama and the managed devices. You can generate these custom certificates locally or import them from an existing enterprise public key infrastructure (PKI). Panorama can manage devices in environments with a mix of predefined and custom certificates.</p> <p>You can also deploy custom certificates for mutual authentication between the firewall and Windows User-ID Agent. This allows the firewall to confirm the Windows User-ID Agent's identity before accepting User-ID information from the agent. Deploy a custom certificate on the Windows User-ID Agent and a certificate profile on the firewall, containing the CA of the certificate, to establish a unique trust chain between the two devices.</p>

New Authentication Features (Continued)	Description
Authentication for External Dynamic Lists	The firewall now validates the digital certificates of SSL/TLS servers that host external dynamic lists, and, if the servers enforce basic HTTP username/password authentication (client authentication), the firewall can forward login credentials to gain access to the lists. If an external dynamic list source fails server or client authentication, the firewall does not retrieve the list and ceases to enforce policy based on its contents. These security enhancements help ensure that the firewall retrieves IP addresses, domains, or URLs from a valid source over a secure, private channel.


## User-ID Features

New User-ID Features	Description
Panorama and Log Collectors as User-ID Redistribution Points	You can now leverage your Panorama and distributed log collection infrastructure to <a href="#">redistribute User-ID mappings</a> in large-scale deployments. By using the existing connections from firewalls to Log Collectors to Panorama, you can aggregate the mappings without setting up and managing extra connections between firewalls.
Centralized Deployment and Management of User-ID and TS Agents	You can now use endpoint management software such as Microsoft SCCM to <a href="#">remotely install, configure, and upgrade</a> multiple Windows-based User-ID agents and Terminal Services (TS) agents in a single operation. Using endpoint management software streamlines your workflow by enabling you to deploy and configure numerous User-ID and TS agents through an automated process instead of using a manual login session for each agent.
User Groups Capacity Increase	To accommodate environments where access control for each resource is based on membership in a user group, and where the number of resources and groups is increasing, you can now <a href="#">reference more groups in policy</a> (the limit varies by platform).
User-ID Syslog Monitoring Enhancements	The following enhancements <a href="#">improve the accuracy of User-ID mappings</a> and simplify monitoring syslog servers for mapping information: <ul style="list-style-type: none"> <li>• Automatic deletion of user mappings—To improve the accuracy of your user-based policies and reports, the firewall can now use syslog monitoring to detect when users have logged out and then delete the associated User-ID mappings.</li> <li>• Multiple syslog formats—In environments with multiple points of authentication sending syslog messages in different formats, it is now easier to monitor login and logout events because the firewall can ingest multiple formats from a syslog server aggregating from various sources.</li> </ul>
Group-Based Reporting in Panorama	Panorama now provides visibility into the activities of <a href="#">user groups</a> in your network through the User Activity report, SaaS Application Usage report (see <a href="#">SaaS Application Visibility for User Groups</a> ), custom reports, and the ACC. Panorama aggregates group activity information from managed firewalls so that you can filter logs and generate reports for all groups.

## App-ID Features

New App-ID Features	Description
SaaS Application Visibility for User Groups	<p>To help you monitor the assortment of SaaS applications that serve the productivity needs of the user groups on your network and ensure the security and data integrity demands for the organization, the SaaS Application Usage PDF report now includes data on user groups. The report highlights the most used applications by user groups and presents the volume of data each user group transfers using sanctioned and unsanctioned applications. For a more granular view, you can customize the report to show application usage for a specific user group, application usage on a specific security zone, and report on application usage by multiple user groups within a security zone.</p> <p>In addition to the enhancements in the PDF report, you can now use the ACC to visualize SaaS activity trends on your network. The ACC includes global filters for viewing SaaS application usage based on risk rating or by the number of sanctioned and unsanctioned applications in use on your network.</p>
ALG Support for IPv6	<p>The firewall can now safely enable Session Initiation Protocol (SIP) and Skinny Client Control Protocol (SCCP) for IPv6 and dual-stack networks. You can safely allow these protocols without opening a wide range of ports to allow the traffic.</p>

## Decryption Features

New Decryption Features	Description
Decryption for Elliptical Curve Cryptography (ECC) Certificates	<p>Firewalls enabled to decrypt SSL traffic now decrypt SSL traffic from websites and applications using ECC certificates, including Elliptical Curve Digital Signature Algorithm (ECDSA) certificates. As some organizations transition to using ECC certificates to take advantage of benefits such as strong keys and small certificate size, this feature ensures that you maintain visibility into and can safely enable ECC-secured application and website traffic.</p> <p> Decryption for websites and applications using ECC certificates is not supported for traffic that is mirrored to the firewall; encrypted traffic using ECC certificates must pass through the firewall directly for the firewall to decrypt it.</p>
Management for Decryption Exclusions	<p>You now have increased flexibility to manage traffic excluded from decryption. New, centralized SSL decryption exclusion management enables you to both create your own custom decryption exclusions, and to review Palo Alto Networks predefined decryption exclusions in a single place:</p> <ul style="list-style-type: none"> <li>• A simplified workflow allows you to easily exclude traffic from decryption based on hostname.</li> <li>• The firewall does not decrypt applications that are known to break during decryption. Now, you can view these decryption exceptions directly on the firewall. Updates and additions to the Palo Alto Networks predefined decryption exclusions are delivered to the firewall in content updates and are enabled by default.</li> </ul>
Perfect Forward Secrecy (PFS) Support with SSL Inbound Inspection	<p>PAN-OS 7.1 introduced PFS for SSL Forward Proxy decryption; now, in PAN-OS 8.0, PFS support is extended to SSL Inbound Inspection. PFS ensures that data from sessions undergoing decryption cannot later be retrieved if server private keys are compromised. You can enforce Diffie-Hellman key exchange-based PFS (DHE) and elliptic curve Diffie-Hellman (ECDHE)-based PFS for decrypted SSL traffic.</p>

## Virtualization Features

New Virtualization Features	Description
<p>VM-Series Firewall Performance Enhancements and Expanded Model Line</p>	<p>This feature introduces <a href="#">improved performance, capacity, and efficiency for all VM-Series firewalls, including three new VM-Series models</a>: VM-50, VM-500, and VM-700. The VM-Series model lineup now covers a wide variety of firewalls—from small optimized firewalls in resource-constrained environments to large, high performance firewalls for deployment in a diverse range of Network Function Virtualization (NFV) use cases. You can also leverage the expanded range of VM-Series models coupled with flexibility and per-tenant isolation of VM-Series models to deploy multi-tenant solutions.</p> <ul style="list-style-type: none"> <li>• VM-50 Firewall—A virtual firewall with an optimized compute resource footprint. This firewall is ideal for use in virtual customer premises equipment (vCPE) and high density multi-tenancy solutions for managed security service providers (MSSP).</li> <li>• VM-500 and VM-700 Firewalls—When utilizing a larger compute resource footprint, these virtual firewalls provide high performance and capacity. The VM-500 and VM-700 firewalls are ideal in NFV use cases for service provider infrastructure and data center roles.</li> <li>• VM-100, VM-200, VM-300, VM-1000-HV Firewalls—Existing VM-Series models now feature increased performance, capacity, and efficiency when compared to the same compute resources in earlier release versions. This release also consolidates the VM-200 with the VM-100 and the VM-1000-HV with the VM-300, which means that the VM-100 and VM-200 are now functionally identical, as are the VM-300 and VM-1000-HV.</li> </ul> <p>In addition, VM-Series firewall models are now distinguished by session capacity and the number of maximum effective vCPU cores (instead of only session capacity).</p>
<p>CloudWatch Integration for the VM-Series Firewall on AWS</p>	<p>VM-Series firewalls on AWS can now <a href="#">natively send PAN-OS metrics to AWS CloudWatch</a> for advanced monitoring and auto-scaling policy decisions. The CloudWatch integration enables you to monitor the capacity, health status, and availability of the firewalls with metrics such as total number of active sessions, GlobalProtect gateway tunnel utilization, or SSL proxy utilization, so that the security tier comprising the VM-Series firewalls can scale dynamically when your EC2 workloads scale in response to demand.</p>
<p>Seamless VM-Series Model Upgrade</p>	<p>This release introduces <a href="#">seamless license capacity upgrades</a> of the VM-Series firewall. If a tenant's requirements increase, you can upgrade the capacity to accommodate the changes with minimal traffic and operation disruption. Additionally, VM-Series firewalls now support HA synchronization between VM-Series firewalls of different capacities during the upgrade process.</p>
<p>VM-Series NSX Integration Configuration through Panorama</p>	<p>The <a href="#">new Panorama VMware NSX plug-in</a> streamlines the process of deploying VM-Series firewall for NSX and eliminates the duplicate effort in defining the security-related configuration on both Panorama and the NSX Manager or vCenter server. Panorama now serves as the single point of configuration that provides the NSX Manager with the contextual information required to redirect traffic from the guest virtual machines to the VM-Series firewall. When you commit the NSX configuration, Panorama generates a security group in the NSX environment for each qualified dynamic address group and Panorama pushes each steering rule generates NSX Manager. The NSX Manager uses the steering rules to redirect traffic from the virtual machines belonging to the corresponding NSX security group.</p>

New Virtualization Features (Continued)	Description
Support for NSX Security Tags on the VM-Series NSX Edition Firewall	The VM-Series firewall can now <a href="#">dynamically tag a guest VM with NSX security tags</a> to enable immediate isolation of compromised or infected guests. The universally unique identifier of a guest VM is now part of the Traffic and Threat logs on the firewall. By leveraging threat, antivirus, and malware detection logs on the VM-Series firewall, NSX Manager can place guests in a quarantined security group to prevent lateral movement of the threat in the virtualized data center environment.
New Serial Number Format for the VM-Series Firewall	The serial number format for the VM-Series firewall now displays the name of the hypervisor on which the firewall is deployed so that you can consistently identify the firewalls for license management, and content and software updates. The new format is 15 characters in length, numeric for the bring your own license (BYOL) model, and alphanumeric for the Marketplace models (Bundle 1 or Bundle 2) available in public cloud environments. As part of this change, VM-Series firewalls in AWS now support longer instance ID formats.
VM-Series Bootstrapping with Block Storage	You can now <a href="#">bootstrap the VM-Series firewall in ESXi, KVM, and Hyper-V using block storage</a> . This option provides a bootstrapping solution for environments where mounting a CD-ROM is not supported.
VM-Series License Deactivation API Key	<p>To deactivate a VM-Series license, you must first install a <a href="#">license deactivation API key</a> on your firewall or Panorama. The deactivation API key provides an additional layer of security for communications between the Palo Alto Networks Update Server and VM-Series firewalls and Panorama. The PAN-OS software uses this API key to authenticate with the update and licensing servers.</p> <p>The API key is available through the Customer Support Portal to administrators with superuser privileges.</p>
Support for VM-Series on Azure Government	Azure Government is a public cloud platform for U.S. government and public sector agencies. The <a href="#">VM-Series firewall on Azure</a> now provides the same robust security features in Azure Government as in the Azure public cloud. On the Azure Government Marketplace, the VM-Series firewall is only available as a bring your own license (BYOL) option because the Azure Government Marketplace does not support pay-as-you-go (PAYG).



## Networking Features

New Networking Features	Description
Tunnel Content Inspection	<p>The firewall can now inspect the traffic content of cleartext tunnel protocols:</p> <ul style="list-style-type: none"> <li>• Generic Routing Encapsulation (GRE)</li> <li>• Non-encrypted IPSec traffic (NULL Encryption Algorithm for IPSec and transport mode AH IPSec)</li> <li>• General Packet Radio Service (GPRS) Tunneling Protocol for User Data (GTP-U)</li> </ul> <p>This enables you to enforce Security, DoS Protection, and QoS policies on traffic in these types of tunnels and traffic nested within another cleartext tunnel (for example, Null Encrypted IPSec inside a GRE tunnel). You can also view tunnel inspection logs and tunnel activity in the ACC to verify that tunneled traffic complies with corporate security and usage policies.</p> <p>The firewall supports <a href="#">tunnel content inspection</a> of GRE and non-encrypted IPSec on all firewall models. It supports tunnel content inspection of GTP-U on PA-5200 Series firewalls and VM-Series firewalls. The firewall is not terminating the GRE, non-encrypted IPSec, or GTP-U tunnel.</p>
Multiprotocol BGP	<p>The firewall now supports <a href="#">Multiprotocol BGP</a> (MP-BGP) so that a firewall enabled with BGP can advertise IPv4 multicast routes and IPv6 unicast routes (in addition to the IPv4 unicast routes it already supports) in BGP Update messages. In this way, MP-BGP provides IPv6 connectivity for your BGP networks that use either native IPv6 or dual stack IPv4 and IPv6. For example, in a service provider environment, you can offer IPv6 service to customers. In an enterprise environment, you can use IPv6 service from service providers. You can also separate your unicast and multicast traffic so they take different paths, in case you need multicast traffic to undergo less latency or take fewer hops.</p>
Static Route Removal Based on Path Monitoring	<p>You can now use <a href="#">path monitoring</a> to determine if a static or default route is down. If path monitoring to one or more monitored destinations fails, the firewall considers the static or default route down and uses an alternative route so that the traffic is not black-holed (silently discarded). Likewise, the firewall advertises an alternative static route (rather than a failed route) for route redistribution into a dynamic routing protocol.</p> <p>You can enable path monitoring on static routes between routers, on static routes where a peer does not support Bidirectional Forwarding Detection (BFD), and on static routes where policy-based forwarding (PBF) path monitoring is insufficient because it does not replace failed routes with alternative routes.</p>
IPv6 Router Advertisement for DNS Configuration	<p>To make DNS resolution easier for your IPv6 hosts, the firewall now has enhanced Neighbor Discovery (ND) so that you can provision IPv6 hosts joining the network with Recursive DNS Server (RDNS) and DNS Search List (DNSSL) options, eliminating the need for a separate DHCPv6 server. The firewall sends <a href="#">IPv6 Router Advertisements</a> with these options; thus, your IPv6 hosts are configured with:</p> <ul style="list-style-type: none"> <li>• The addresses of RDNS servers that can resolve DNS queries.</li> <li>• A list of the domain names (suffixes) that the DNS client appends (one at a time) to an unqualified domain name before entering the domain name into a DNS query.</li> </ul>
NDP Monitoring for Fast Device Location	<p>You can now enable <a href="#">Neighbor Discovery Protocol (NDP) monitoring</a> for a dataplane interface on the firewall so that you can view the IPv6 addresses of devices on the link local network, their corresponding MAC address, and username from User-ID (if the user of that device uses the directory service to log in). Having these three pieces of information in one place about a device that violates a security rule allows you to quickly track the device. You can also monitor IPv6 ND logs to make troubleshooting easier.</p>



New Networking Features	Description
Zone Protection for Non-IP Protocols on a Layer 2 VLAN or Virtual Wire	You can now whitelist or blacklist non-IP protocols between security zones or between interfaces within a security zone in a Layer 2 VLAN or on a virtual wire. The firewall normally passes non-IP protocols between Layer 2 zones and between virtual wire zones; with this feature, you can now <a href="#">control non-IP protocols</a> between these zones. For example, if you don't want legacy Windows XP hosts to discover other NetBEUI-enabled hosts on another zone, you can configure a Zone Protection profile to blacklist NetBEUI on the ingress zone.
Global and Zone Protection for Multi-path TCP (MPTCP) Evasions	You can now enable or disable <a href="#">Multi-path TCP (MPTCP)</a> globally or for each network zone. MPTCP is an extension of TCP that allows a client to simultaneously use multiple paths (instead of a single path) to connect with a destination host. MPTCP especially benefits mobile users, enabling them to maintain dual connections to both Wi-Fi and cellular networks as they move—this improves both the resilience and quality of the mobile connection and enhances the user experience. However, MPTCP can also potentially be leveraged by attackers as part of an evasion technique. This feature provides the flexibility to enable or disable MPTCP for all firewall traffic or for individual network zones, based on the visibility, performance, and security requirements for each network zone.
Zone Protection for SYN Data Payloads	<p>You can now drop <a href="#">TCP SYN and SYN-ACK packets</a> that contain data in the payload during a three-way handshake. In case the payload is malicious—for example if it contains command and control traffic or it is being used to exfiltrate data—dropping such packets can prevent successful attacks.</p> <p>The TCP Fast Open option preserves the speed of a connection setup by including data in the payload of SYN and SYN-ACK packets. The Zone Protection profile treats TCP handshakes that use the Fast Open option separately from other SYN and SYN-ACK packets; the profile is set to allow the handshake packets if they contain a valid Fast Open cookie.</p>
Hardware IP Address Blocking	When you configure the firewall with a DoS Protection policy or Vulnerability Protection profile to <a href="#">block packets</a> from specific IPv4 addresses, the firewall now automatically blocks that traffic in hardware before those packets use CPU or packet buffer resources. Blocking traffic by default in hardware allows the firewall to stop DoS attacks even faster than blocking traffic in software. If the amount of attack traffic exceeds the hardware block capacity, IP blocking mechanisms in software block the excess traffic. This feature is supported on PA-3060 firewalls, PA-3050 firewalls, PA-5000 Series, PA-5200 Series, and PA-7000 Series firewall models.
Packet Buffer Protection	<a href="#">Packet buffer protection</a> allows you to protect the firewall from being impacted by single source denial of service (DoS) attacks. These attacks come from sessions or IP addresses that are not blocked by Security policy. After a session is permitted by the firewall, it can generate such a high volume of traffic that it overwhelms the firewall packet buffer and causes the firewall to appear to hang as both attack and legitimate traffic are dropped. The firewall tracks the top packet buffer consumers and gives you the ability to configure global thresholds that specify when action is taken against these sessions. After identifying a session as abusive, the firewall uses Random Early Drop (RED) as a first line of defense to throttle the offending session and then discards the session if the abuse continues. If a particular IP address creates many sessions that are discarded, the firewall blocks it.
Reconnaissance Protection Source Address Exclusion	Zone protection's reconnaissance protection detects and takes action against host sweep and TCP and UDP port scans. This is useful against attackers searching for vulnerabilities. However, it can also negatively impact scanning activities, such as network security testing or fingerprinting. You can now <a href="#">whitelist source addresses to exclude them from reconnaissance protection</a> . This allows you to protect your network from reconnaissance attacks while allowing legitimate monitoring tools.

New Networking Features	Description
IKE Peer and IPSec Tunnel Capacity Increases	The PA-7000 Series, PA-5000 Series, and PA-3000 Series models now support <a href="#">more IKE peers and IPSec tunnels</a> than in prior releases. This is a benefit in service provider and large enterprise environments where you need to support many site-to-site VPN peers and IPSec VPN connections between remote sites.

## GlobalProtect Features

New GlobalProtect Features	Description
IPv6 for GlobalProtect	GlobalProtect clients and satellites can now connect to portals and gateways using <a href="#">IPv6</a> . This feature allows connections from clients that are in IPv6-only environments, IPv4 only environments, or dual-stack (IPv4 and IPv6) environments. You can tunnel IPv4 traffic over an IPv6 tunnel and the IP address pool can assign both IPv4 and IPv6 addresses. To use this feature, you must install a GlobalProtect subscription on each gateway that supports GlobalProtect clients that use IPv6 addresses.
Clientless SSL VPN	<a href="#">Clientless VPN</a> , which provides secure remote access to common enterprise web applications that use HTML, HTML5, and JavaScript technologies, is now available in <i>public beta</i> . Users have the advantage of secure access from SSL-enabled web browsers without installing GlobalProtect client software. This is useful when you need to enable partner or contractor access to applications, and to safely enable unmanaged assets, including personal devices. You can configure the GlobalProtect portal landing page to provide access to web applications based on users and user groups and also allow single-sign on to SAML-enabled applications. Supported operating systems are Windows, Mac, iOS, Android, Chrome, and Linux. Supported browsers are Chrome, Internet Explorer, Safari, and Firefox. This feature requires you to install a GlobalProtect subscription on the firewall that hosts the Clientless VPN from the GlobalProtect portal.
Define Split Tunnels by Excluding Access Routes	You can now <a href="#">exclude specific destination IP subnets traffic</a> from being sent over the VPN tunnel. With this feature, you can send latency-sensitive or high-bandwidth-consuming traffic outside of the VPN tunnel while all other traffic is routed through the VPN for inspection and policy enforcement by the GlobalProtect gateway.
External Gateway Priority by Source Region	GlobalProtect can now use the geographic region of the GlobalProtect client to determine the best external gateway. <a href="#">Including source region</a> as part of external gateway selection logic, you can ensure that users connect to gateways that are preferred for their current region. This can help avoid distant connections when there are momentary fluctuations of network latency. This can also be used to ensure all connections stay within a region if desired.
Internal Gateway Selection by Source IP Address	GlobalProtect can now <a href="#">restrict internal gateway connection choices based on the source IP address</a> of the client. In a distributed enterprise, this feature allows you to have users from a branch to authenticate and send HIP reports to the firewall configured as the internal gateway for that branch as opposed to authenticating and sending HIP reports to all branches.

New GlobalProtect Features (Continued)	Description
GlobalProtect Agent Login Enhancement	To <a href="#">simplify GlobalProtect agents</a> and prevent unnecessary login prompts when a username and password are not required, the panel that showed portal, username, and password is now split into two screens (one screen for the portal address and another screen for username and password). The GlobalProtect agent now displays login prompts for username and password only if this information is required. GlobalProtect automatically hides the username and password screen for authentication types—such as cookie or client certificate authentication—that do not require a username and password.
Authentication Policy and Multi-Factor Authentication for GlobalProtect	You can leverage the new <a href="#">Authentication Policy and Multi-Factor Authentication</a> enhancements <a href="#">within GlobalProtect</a> to support access to non-HTTP applications that require multi-factor authentication. GlobalProtect can now notify and prompt the user to perform the timely, multi-factor authentication needed to access sensitive network resources.
SAML 2.0 Authentication for GlobalProtect	GlobalProtect portals, gateways, and clients now support <a href="#">SAML 2.0 Authentication</a> . If you have chosen SAML as your authentication standard, GlobalProtect portals and gateways can <a href="#">act as Security Assertion Markup Language (SAML) 2.0 service providers</a> and GlobalProtect clients can authenticate users directly to the SAML identity provider.
Restrict Transparent Agent Upgrades to Internal Network Connections	You can now <a href="#">control when transparent upgrades occur</a> for a GlobalProtect client. With this configuration, if the user connects from outside the corporate network, the upgrade is postponed. Later, when the user connects from within the corporate network, the upgrade is activated. This feature allows you to hold the updates until users can take advantage of good network availability and high bandwidth from within the corporate network. The upgrades will not hinder users when they travel to environments with low bandwidth.
<a href="#">AirWatch MDM Integration</a>	The PAN-OS Windows User-ID agent has been extended to support a new <a href="#">AirWatch MDM Integration</a> service. This service acts a replacement for the GlobalProtect Mobile Security Manager and enables GlobalProtect to use the host information collected by the service to enforce HIP-based policies on devices managed by VMware AirWatch. Running as part of the PAN-OS Windows User-ID agent, the AirWatch MDM integration service uses the AirWatch API to collect information from mobile devices (including Android and iOS) that are managed by AirWatch and translate this data into host information.
Increased Capacity for Split Tunnel Include Access Routes	In PAN-OS 8.0.2, the firewall now supports up to 1000 access routes used to include traffic in a split tunnel gateway configuration. This enables you include a greater number of routes from being sent over the GlobalProtect VPN tunnel than was previously available. Note that the exclude tunnel capacity remains the same at 200 access routes. For upgrade and downgrade considerations for this feature, see in the <a href="#">PAN-OS 8.0 New Features Guide</a> .


## Changes to Default Behavior

The following topics describe changes to default behavior in PAN-OS and Panorama 8.0:

- ▲ [Authentication Changes](#)
- ▲ [Content Inspection Changes](#)
- ▲ [GlobalProtect Changes](#)
- ▲ [Management Changes](#)
- ▲ [Panorama Changes](#)
- ▲ [VM-Series Firewall Changes](#)
- ▲ [WildFire Changes](#)

### Authentication Changes

PAN-OS 8.0 has the following changes in default behavior for authentication features:

Feature	Change
Hardware security modules	 (PAN-OS 8.0.2 and later releases) To downgrade to a release earlier than PAN-OS 8.0.2, you must ensure that the master key is stored locally on Panorama or on the firewall, not on a hardware security module (HSM).
Authentication policy	Authentication policy replaces Captive Portal policy.
Logging	When an authentication event invokes a policy rule, the firewall now generates Authentication logs instead of System logs.
RADIUS and TACACS+	You now use the web interface instead of a CLI command to set the authentication protocol to CHAP or PAP for TACACS+ and RADIUS server profiles.

### Content Inspection Changes

PAN-OS 8.0 has the following changes in default behavior for content inspection features:

Feature	Change
TCP settings	<p>The defaults for the following TCP Settings (<b>Device &gt; Setup &gt; Session &gt; TCP Settings</b>) have been changed in 8.0:</p> <ul style="list-style-type: none"> <li>• <b>Drop segments without flag</b> is now enabled by default. The corresponding CLI command, <code>set deviceconfig setting tcp drop-zero-flag</code> is now set to <code>yes</code> by default.</li> <li>• <b>Drop segments with null timestamp option</b> is now enabled by default. The corresponding CLI command, <code>set deviceconfig setting tcp check-timestamp-option</code> is now set to <code>yes</code> by default.</li> <li>• <b>Forward segments exceeding TCP out-of-order queue</b> is now disabled by default. The corresponding CLI command, <code>set deviceconfig setting bypass-exceed-op-queue</code> is now set to <code>no</code> by default.</li> </ul>
Content-ID	<p><b>Forward segments exceeding TCP App-ID inspection queue (Device &gt; Setup &gt; Content-ID &gt; Content-ID Settings)</b> is now disabled by default. The corresponding CLI command, <code>set deviceconfig setting application bypass-exceed-queue</code> is now set to <code>no</code> by default.</p>
Zone Protection profiles	<p>In a Zone Protection profile for Packet Based Attack Protection, the default setting is now to drop TCP SYN and SYN-ACK packets that contain data in the payload during a three-way handshake. (In prior PAN-OS releases, firewall allowed such packets.) By default, a Zone Protection profile is set to allow TCP handshake packets that use the TCP Fast Open option if they contain a valid Fast Open cookie. If you have existing Zone Protection profiles in place when you upgrade to PAN-OS 8.0, the three default settings will apply to each profile and the firewall will act accordingly.</p>
Decryption	<p>The firewall does not support SSL decryption of RSA keys that exceed 8Kb in size. You can either block connections to servers that use certificates with RSA keys exceeding 8Kb or skip SSL decryption for such connections. To block such connections, select <b>Objects &gt; Decryption Profile</b>, edit the profile, select <b>SSL Decryption &gt; SSL Forward Proxy</b>, and in the Unsupported Mode Checks section select <b>Block sessions with unsupported cipher suites</b>. To skip decryption for such connections, clear <b>Block sessions with unsupported cipher suites</b>.</p>
URL Filtering	<p>When a firewall running PAN-OS 8.0 connects with PANDB (public or private cloud), it validates the Common Name on the server certificate before establishing an SSL connection. If the validation fails, the connection is refused and the firewall generates a system log.</p>
Data Pattern objects	<p><b>Objects &gt; Custom Objects &gt; Data Patterns</b> provides predefined patterns (<b>Pattern Type &gt; Predefined Pattern</b>), such as social security numbers and credit card numbers, to check for in the incoming file types that you specify. The firewall no longer supports checking for these predefined patterns in GZIP and ZIP files.</p>

## GlobalProtect Changes

PAN-OS 8.0 has the following changes in default behavior for GlobalProtect features:

Feature	Change												
GlobalProtect portals	<ul style="list-style-type: none"> <li>The <b>Agent &gt; Gateways</b> tab for GlobalProtect portal configurations is split into two separate tabs: <b>Internal</b> and <b>External</b>. Use the <b>Internal</b> tab to specify internal gateway settings for GlobalProtect agents and apps. Use the <b>External</b> tab to specify external gateway settings for GlobalProtect agents and apps. These are layout changes only—your existing PAN-OS 7.1 configuration is preserved.</li> <li>The <b>Disable login page</b> check box on the <b>General</b> tab for GlobalProtect portal configurations is now a <b>Disable</b> command in the <b>Portal Login Page</b>. This is a layout change only—your existing PAN-OS 7.1 configuration is preserved.</li> </ul>												
GlobalProtect gateways	The <b>Agent &gt; Client Settings &gt; Network Settings</b> tab for GlobalProtect gateway configurations is replaced with two separate tabs: <b>IP Pools</b> and <b>Split Tunnel</b> . These are layout changes only—your existing PAN-OS 7.1 configuration is preserved.												
IP address pools	In PAN-OS 7.1 and earlier releases, to prevent potential IP address conflicts, the GlobalProtect gateway did not assign an IP address if the local network IP address sent from the endpoint was in the same subnet as the IP address pool. Users had to configure a second IP address pool that contained addresses from a separate subnet. Beginning in PAN-OS 8.0, when you configure only one IP address pool, GlobalProtect assigns an IP address regardless of subnet overlap. This change may cause warning messages on Windows endpoints. If you are concerned about the warning message, configure a second IP address pool.												
Clientless VPN	The option to <b>Allow user to launch unpublished applications</b> is now renamed <b>Display application URL address bar</b> . The new option name better reflects the purpose of this option.												
Web interfaces changes	GlobalProtect has the following minor changes to menu and check box labels. These are changes to wording only—your existing PAN-OS 7.1 configuration is preserved.												
	<table border="1"> <thead> <tr> <th>Location</th> <th>PAN-OS 7.1 Label</th> <th>PAN-OS 8.0 Label</th> </tr> </thead> <tbody> <tr> <td>The <b>General</b> tab for GlobalProtect portal configurations</td> <td>Custom Login Page</td> <td>Portal Login Page</td> </tr> <tr> <td>The <b>General</b> tab for GlobalProtect portal configurations</td> <td>Custom Help Page</td> <td>App Help Page</td> </tr> <tr> <td>The <b>Agent &gt; External &gt; Add &gt; External Gateway</b> for GlobalProtect portal configurations</td> <td>If this GlobalProtect gateway can be manually selected</td> <td>Manual (the user can manually select this gateway)</td> </tr> </tbody> </table>	Location	PAN-OS 7.1 Label	PAN-OS 8.0 Label	The <b>General</b> tab for GlobalProtect portal configurations	Custom Login Page	Portal Login Page	The <b>General</b> tab for GlobalProtect portal configurations	Custom Help Page	App Help Page	The <b>Agent &gt; External &gt; Add &gt; External Gateway</b> for GlobalProtect portal configurations	If this GlobalProtect gateway can be manually selected	Manual (the user can manually select this gateway)
	Location	PAN-OS 7.1 Label	PAN-OS 8.0 Label										
	The <b>General</b> tab for GlobalProtect portal configurations	Custom Login Page	Portal Login Page										
The <b>General</b> tab for GlobalProtect portal configurations	Custom Help Page	App Help Page											
The <b>Agent &gt; External &gt; Add &gt; External Gateway</b> for GlobalProtect portal configurations	If this GlobalProtect gateway can be manually selected	Manual (the user can manually select this gateway)											

## Management Changes

PAN-OS 8.0 has the following changes in default behavior for firewall and Panorama management features:

Feature	Change
Management access	<ul style="list-style-type: none"> <li>By default, the firewall and Panorama no longer allow management access over TLSv1.0 connections. If you accept this default, any scripts that require management access (such as API scripts) must support TLSv1.1 or later TLS versions. To overcome the default restriction, you can <a href="#">configure an SSL/TLS service profile</a> that allows TLSv1.0 and assign the profile to the interface used to access the firewall or Panorama.</li> <li>To configure the management (MGT) interface on the firewall, you now select <b>Device &gt; Setup &gt; Interfaces</b> instead of <b>Device &gt; Setup &gt; Management</b>.</li> </ul>
Configuration backups	To create a snapshot file for the candidate configuration, you must now select <b>Config &gt; Save Changes</b> instead of <b>Save</b> at the top right of the web interface.
External dynamic lists	<ul style="list-style-type: none"> <li>When retrieving an external dynamic list from a source with an HTTPS URL, the firewall now authenticates the digital certificates of the list source. You must configure a certificate profile to authenticate the source. If the source authentication fails, the firewall stops enforcing policy based on the list contents.</li> <li>In PAN-OS 7.1, the firewall supported a maximum of 30 unique sources for external dynamic lists and enforced the maximum number even if the external dynamic list was not used in policy. Beginning in PAN-OS 8.0, only the lists you use to enforce policy will count toward the maximum number allowed.</li> <li>Entries in an external dynamic list (IP addresses, domains, and URLs) now only count toward the maximum number that the firewall supports if a security policy rule references the external dynamic list.</li> </ul>
Anti-Spyware profiles	In PAN-OS 7.1 and earlier releases, passive DNS monitoring was a setting you could enable in an Anti-Spyware Profile. You could attach the Anti-Spyware Profile to a policy rule and then sessions that match that rule will trigger passive DNS monitoring. Beginning in PAN-OS 8.0, passive DNS monitoring is a global setting that you can enable through the Telemetry and Threat Intelligence feature, and when enabled, the firewall acts as a passive DNS sensor for all traffic that passes through the firewall.
Service routes	The firewall now uses the new service route <b>Palo Alto Networks Services</b> to access external services that it accessed via the service routes <b>Palo Alto Updates</b> and <b>WildFire Public</b> prior to PAN-OS 8.0.
Content and software updates	Beginning with PAN-OS 8.0, the <b>Verify Update Server Identity</b> global services setting for installing content and software updates is enabled by default ( <b>Device &gt; Setup &gt; Services &gt; Global</b> ).

## Panorama Changes

PAN-OS 8.0 has the following changes in default behavior for Panorama features:

Feature	Change
Management access	To configure interfaces on Panorama, you now select <b>Panorama &gt; Setup &gt; Interfaces</b> (instead of <b>Panorama &gt; Setup &gt; Management</b> ).

Feature	Change
Log collection	<ul style="list-style-type: none"> <li>When adding or editing a Log Collector (<b>Panorama &gt; Managed Collectors</b>), you now configure interfaces in the <b>Interfaces</b> tab, which replaces the <b>Management</b>, <b>Eth1</b>, and <b>Eth2</b> tabs in the Collector dialog.</li> <li>When the Panorama virtual appliance is in Panorama mode and is deployed in a high availability (HA) configuration, you can configure both HA peers to collect logs, not just the active peer.</li> </ul>
Commit and push operations	When pushing configurations to managed firewalls or Log Collectors, Panorama now pushes the running configuration instead of the candidate configuration. Therefore, you must commit changes to Panorama before pushing the changes to firewalls or Log Collectors.
Content and software updates	Firewalls and Log Collectors now retrieve software and content updates from Panorama over port 28443 instead of Panorama pushing the updates over port 3978.

## VM-Series Firewall Changes

PAN-OS 8.0 has the following changes in default behavior for VM-Series firewalls:

Feature	Change
Management interfaces	In PAN-OS 8.0, the use of hypervisor-assigned MAC addresses and DHCP on management interfaces are enabled on new VM-Series firewall installations. These options are not enabled automatically when upgrading a VM-Series firewall to PAN-OS 8.0 from PAN-OS 7.1 or earlier releases.
Licensing	Beginning with PAN-OS 7.1.7, to deactivate a VM-Series license you must first install a license API key on your firewall or Panorama. For more information, see <a href="#">Virtualization Features</a> .
Large Receive Offload	Large Receive Offload (LRO) is enabled by default on the new deployments of the VM-Series firewall for NSX or deployments upgraded to 8.0.
Data Plane Development Kit	Support for Data Plane Development Kit (DPDK) is enabled by default on the VM-Series for KVM and ESXi. However, to take advantage of DPDK, you must install the required NIC driver on your hypervisor. DPDK support is disabled by default on the VM-Series for AWS.

## WildFire Changes

PAN-OS 8.0 has the following changes in default behavior for WildFire features:



Feature	Change
Logging	<ul style="list-style-type: none"><li>• If you previously enabled WildFire forwarding on your firewall, the firewall now forwards blocked files that match existing signatures, in addition to unknown files, for WildFire analysis. The WildFire Submissions log now includes log entries for blocked files.</li><li>• The Action column in the WildFire Submissions log now indicates if the firewall action for a sample was <b>allow</b> or <b>block</b>. In PAN-OS 7.1 and earlier versions, the action displayed for all samples in the WildFire Submissions log was <b>alert</b>.</li></ul>
DoS Protection profiles	When you use a Classified DoS Protection profile for flood protection or a Vulnerability Protection profile that is configured to Block IP addresses, the firewall will now block IP addresses in hardware first, and then in software if the hardware block list has reached its capacity.

## CLI and XML API Changes in PAN-OS 8.0

PAN-OS 8.0 has changes to existing CLI commands, which also affect corresponding PAN-OS XML API requests. If you have a script or application that uses these requests, [run corresponding CLI commands in debug mode](#) to view the corresponding XML API syntax.

Operational commands are preceded by a greater-than sign (>), while configuration commands are preceded by a hash (#). An asterisk (\*) indicates that related commands in the same hierarchy have also changed.

- ▲ [Authentication CLI Changes](#)
- ▲ [Content Inspection CLI Changes](#)
- ▲ [GlobalProtect CLI Changes](#)
- ▲ [Management CLI Changes](#)
- ▲ [User-ID CLI Changes](#)

### Authentication CLI Changes

PAN-OS 8.0 has the following CLI and XML API changes for Authentication features:

Feature	Change
Authentication policy	<p>With Authentication policy replacing Captive Portal policy, the related CLI commands have changed:</p> <ul style="list-style-type: none"> <li>• <b>PAN-OS 7.1 and earlier releases:</b> <pre>&gt; show running captive-portal-policy &gt; test cp-policy-match * # show rulebase captive-portal * # set import resource max-cp-rules &lt;0-4000&gt; # set rulebase captive-portal * # set shared admin-role &lt;name&gt; role device webui policies captive-portal-rulebase &lt;enable read-only disable&gt; # set import resource max-cp-rules &lt;0-4000&gt;</pre> </li> <li>• <b>PAN-OS 8.0 release:</b> <pre>&gt; show running authentication-policy &gt; test authentication-policy-match * # show rulebase authentication * # set import resource max-auth-rules &lt;0-4000&gt; # set rulebase authentication rules * # set shared admin-role &lt;name&gt; role device webui policies authentication-rulebase &lt;enable read-only disable&gt; # set import resource max-auth-rules &lt;0-4000&gt;</pre> </li> </ul>

Feature	Change
Certificate management	<p>With the introduction of decryption for Elliptical Curve Cryptography (ECC) Certificates, the following CLI command has been replaced with two algorithm-specific commands:</p> <ul style="list-style-type: none"> <li>• <b>PAN-OS 7.1 and earlier releases:</b> <pre># set deviceconfig setting ssl-decrypt fwd-proxy-server-cert-key-size &lt;0 1024 2048&gt;</pre> </li> <li>• <b>PAN-OS 8.0 release:</b> <pre># set deviceconfig setting ssl-decrypt fwd-proxy-server-cert-key-size-rsa &lt;0 1024 2048&gt; # set deviceconfig setting ssl-decrypt fwd-proxy-server-cert-key-size-ecdsa &lt;0 256 384&gt;</pre> </li> </ul>
Hardware security modules	<p>CLI commands related to SafeNet Network HSM (formerly Luna SA) now reflect the new name:</p> <ul style="list-style-type: none"> <li>• <b>PAN-OS 7.1 and earlier releases:</b> <pre># show deviceconfig system hsm-settings provider safenet-luna-sa * # set deviceconfig system hsm-settings provider safenet-luna-sa *</pre> </li> <li>• <b>PAN-OS 8.0 release:</b> <pre># show deviceconfig system hsm-settings provider safenet-network * # set deviceconfig system hsm-settings provider safenet-network *</pre> </li> </ul>

## Content Inspection CLI Changes

PAN-OS 8.0 has the following CLI and XML API changes for content inspection features:

Feature	Change
Malicious IP address feeds	<p>With new support for malicious IP address feeds, related CLI commands have changed to support IP addresses, URLs, and domains:</p> <ul style="list-style-type: none"> <li>• <b>PAN-OS 7.1 and earlier releases:</b> <pre># set external-list &lt;name&gt; *</pre> </li> <li>• <b>PAN-OS 8.0 release:</b> <pre># set external-list &lt;name&gt; type ip * # set external-list &lt;name&gt; type predefined-ip * # set external-list &lt;name&gt; type domain * # set external-list &lt;name&gt; type url *</pre> </li> </ul>

## GlobalProtect CLI Changes

PAN-OS 8.0 has the following CLI and XML API changes for GlobalProtect features:

Feature	Change
IPv6 support	<p>With the introduction of IPv6 support in GlobalProtect, the following CLI commands have been replaced with two protocol-specific commands:</p> <ul style="list-style-type: none"> <li> <b>PAN-OS 7.1 and earlier releases:</b> <pre># set global-protect global-protect-portal &lt;name&gt; portal-config local-address ip &lt;value&gt;</pre> </li> <li> <b>PAN-OS 8.0 release:</b> <pre># set global-protect global-protect-portal &lt;name&gt; portal-config local-address ip ipv4 &lt;value&gt; # set global-protect global-protect-portal &lt;name&gt; portal-config local-address ip ipv6 &lt;value&gt;</pre> </li> <li> <b>PAN-OS 7.1 and earlier releases:</b> <pre># set global-protect global-protect-portal &lt;name&gt; portal-config local-address floating-ip &lt;value&gt;</pre> </li> <li> <b>PAN-OS 8.0 release:</b> <pre># set global-protect global-protect-portal &lt;name&gt; portal-config local-address floating-ip ipv4 &lt;value&gt; # set global-protect global-protect-portal &lt;name&gt; portal-config local-address floating-ip ipv6 &lt;value&gt;</pre> </li> </ul>

## Management CLI Changes

PAN-OS 8.0 has the following CLI and XML API changes for firewall and Panorama management features:

Feature	Change
Log forwarding	<p>With the introduction of selective log forwarding based on log attributes, you must now specify the name of a custom-filter match list in related CLI commands:</p> <ul style="list-style-type: none"> <li> <b>PAN-OS 7.1 and earlier releases:</b> <pre># show shared log-settings system * # set shared log-settings system * # show shared log-settings config * # set shared log-settings config * # show shared log-settings hipmatch * # set shared log-settings hipmatch * # show shared log-settings profiles &lt;name&gt; * # set shared log-settings profiles &lt;name&gt; *</pre> </li> <li> <b>PAN-OS 8.0 release:</b> <pre># show shared log-settings system match-list * # set shared log-settings system match-list * # show shared log-settings config match-list * # set shared log-settings config match-list * # show shared log-settings hipmatch match-list * # set shared log-settings hipmatch match-list * # show shared log-settings profiles &lt;name&gt; match-list * # set shared log-settings profiles &lt;name&gt; match-list *</pre> </li> </ul>

## User-ID CLI Changes

PAN-OS 8.0 has the following CLI and XML API changes for User-ID features:

Feature	Change
IP address-to-username mapping	<ul style="list-style-type: none"> <li>• The operational command to clear User-ID mappings for all IP addresses or a specific IP address has changed:               <ul style="list-style-type: none"> <li>• <b>PAN-OS 7.1 and earlier releases:</b> <pre>&gt; clear user-cache [all   ip]</pre> </li> <li>• <b>PAN-OS 8.0 release:</b> <pre>&gt; clear ipuser-cache [all   ip]</pre> </li> </ul> </li> <li>• The User-ID commands to clear user mappings from the dataplane have changed:               <ul style="list-style-type: none"> <li>• <b>PAN-OS 7.1 and earlier releases:</b> <pre>&gt; clear uid-gids-cache uid &lt;1-2147483647&gt; &gt; clear uid-gids-cache all</pre> </li> <li>• <b>PAN-OS 8.0 release:</b> <pre>&gt; clear uid-cache uid &lt;1-2147483647&gt; &gt; clear uid-cache all</pre> </li> </ul> </li> </ul>
PAN-OS integrated User-ID agent	<p>CLI commands related to configuring the User-ID agent must now include host-port:</p> <ul style="list-style-type: none"> <li>• <b>PAN-OS 7.1 and earlier releases:</b> <pre># set user-id-agent &lt;name&gt; host &lt;ip/netmask&gt; &lt;value&gt; # set user-id-agent &lt;name&gt; port &lt;1-65535&gt; # set user-id-agent &lt;name&gt; ntlm-auth &lt;yes no&gt; # set user-id-agent &lt;name&gt; ldap-proxy &lt;yes no&gt; # set user-id-agent &lt;name&gt; collectorname &lt;value&gt; # set user-id-agent &lt;name&gt; secret &lt;value&gt;</pre> </li> <li>• <b>PAN-OS 8.0 release:</b> <pre># set user-id-agent &lt;name&gt; host-port host &lt;ip/netmask&gt; &lt;value&gt; # set user-id-agent &lt;name&gt; host-port port &lt;1-65535&gt; # set user-id-agent &lt;name&gt; host-port ntlm-auth &lt;yes no&gt; # set user-id-agent &lt;name&gt; host-port ldap-proxy &lt;yes no&gt; # set user-id-agent &lt;name&gt; host-port collectorname &lt;value&gt; # set user-id-agent &lt;name&gt; host-port secret &lt;value&gt;</pre> </li> </ul>



## Associated Software and Content Versions

The following minimum software versions are supported with PAN-OS 8.0. To see a list of the next-gen firewall models that support PAN-OS 8.0, see the [Palo Alto Networks® Compatibility Matrix](#).

Palo Alto Networks Software or Content Release Version	Minimum Supported Version with PAN-OS 8.0
Panorama	8.0
User-ID Agent	8.0
Terminal Services (TS) Agent	8.0
GlobalProtect Agent	4.0
Applications and Threat Content Release Version	655
Antivirus Content Release Version	2137

## Limitations

The following table includes limitations associated with the PAN-OS 8.0 release.

Issue ID	Description
PAN-68997	<p>The WildFire appliance cluster membership list may not be accurate if cluster members are offline or the membership list is stale. You can import a configuration from any WildFire appliance or appliance cluster into Panorama, add any connected WildFire appliance to a cluster, and assign it a role in the cluster so that you have more flexibility when configuring and re-configuring clusters.</p> <p>After you import a cluster configuration, you can view the cluster members from the Panorama web interface (<b>Panorama &gt; Managed Wildfire Clusters</b>). Check the cluster membership list to ensure that all listed members are nodes in the cluster. Add missing nodes to the cluster as needed.</p> <p>If you import a WildFire appliance that is already part of a cluster or you import a WildFire appliance and later add it to a cluster using local configuration, the Panorama web interface displays it as a standalone appliance and shows it to be out of sync. To resolve this issue, add the node to the cluster, which syncs the configurations in Panorama.</p> <p>To avoid an inaccurate membership list, before you add a node to a cluster, make sure that any WildFire appliance you add to the cluster is not a member of another cluster.</p> <p> Controller and controller backup nodes perform critical cluster management tasks. If you change the controller or controller backup node, ensure that the replacement node is a cluster member. If you inadvertently add a node to more than one cluster, or if you specify a controller or controller backup node that does not belong to the cluster, the consequences vary depending on whether you push the changes to the clusters.</p> <p> If you did not yet commit the changes on the Panorama appliance, or if you only committed the changes but did not push them yet, then first reconfigure the cluster and <b>Commit</b> to Panorama to avoid unintended consequences.</p> <p>If you push a misconfiguration to clusters, cluster behavior is unpredictable and can affect more than one cluster if the pushed Panorama configuration includes nodes that are assigned to more than one cluster. If you inadvertently add a node to more than one cluster, make the appropriate change to correct the misconfiguration:</p> <ul style="list-style-type: none"> <li>• If you have not committed the configuration on Panorama, remove the node from the cluster.</li> <li>• If you have already committed the changes on Panorama, remove the node from the cluster and re-commit the changes to Panorama.</li> <li>• If you have already committed the changes on Panorama and pushed the changes to managed WildFire appliance clusters, remove the node from the cluster, and then re-commit to Panorama and re-push to the WildFire appliance clusters.</li> </ul> <p>If you inadvertently specify a controller or controller backup node that is not a cluster member, make the appropriate change to correct the misconfiguration:</p> <ul style="list-style-type: none"> <li>• If you have not committed the configuration on Panorama, specify a valid cluster node as the controller or controller backup node.</li> <li>• If you have already committed the changes on Panorama, specify a valid cluster node as the controller or controller backup node and <b>Commit to Panorama</b>.</li> <li>• If you have already committed the changes on Panorama and pushed the changes to managed WildFire appliance clusters, specify a valid cluster node as the controller or controller backup node, and then re-commit to Panorama and re-push to the WildFire appliance clusters.</li> </ul>

# Known Issues

The following topics describe known issues in PAN-OS 8.0 releases.



For recent updates to known issues for a given PAN-OS release, refer to <https://live.paloaltonetworks.com/t5/Articles/Critical-Issues-Addressed-in-PAN-OS-Releases/ta-p/52882>.


- ▲ [Known Issues Related to PAN-OS 8.0 Releases](#)
- ▲ [Known Issues Specific to the WF-500 Appliance](#)

## Known Issues Related to PAN-OS 8.0 Releases

The following list includes known issues specific to PAN-OS 8.0 releases, which includes known issues specific to Panorama and GlobalProtect, as well as known issues that apply more generally or that are not identified by an issue ID. See also the [Known Issues Specific to the WF-500 Appliance](#).

Issue ID	Description
–	Upgrading a PA-200 or PA-500 firewall to PAN-OS 8.0 can take 30-60 minutes to complete. Ensure uninterrupted power to your firewall throughout the upgrade process.
GPC-2742	<p>If you configure GlobalProtect portals and gateways to use client certificates and LDAP as two factors of authentication, Chromebook users that are running Chrome OS 47 or later versions can encounter excessive prompts to select a client certificate.</p> <p><b>Workaround:</b> To prevent excessive prompts, configure a policy to specify the client certificate in the Google Admin console and deploy that policy to your managed Chromebooks:</p> <ol style="list-style-type: none"> <li>1. Log in to the Google Admin console (<a href="https://admin.google.com">https://admin.google.com</a>) and select <b>Device management &gt; Chrome management &gt; User settings</b>.</li> <li>2. In the Client Certificates section, enter the following URL pattern to <b>Automatically Select Client Certificate for These Sites</b>:  <pre>{""pattern"": ""https://[*.]"", ""filter"":{}}</pre> </li> <li>3. Click <b>Save</b>. The Google Admin console deploys the policy to all devices within a few minutes.</li> </ol>
GPC-1737	<p>By default, the GlobalProtect app adds a route on iOS mobile devices that causes traffic to the GP-100 GlobalProtect Mobile Security Manager to bypass the VPN tunnel.</p> <p><b>Workaround:</b> To configure the GlobalProtect app on iOS mobile devices to route all traffic—including traffic to the GP-100 GlobalProtect Mobile Security Manager—to pass through the VPN tunnel, perform the following tasks on the firewall hosting the GlobalProtect gateway (<b>Network &gt; GlobalProtect &gt; Gateways &gt; &lt;gateway-config&gt; &gt; Agent &gt; Client Settings &gt; &lt;client-settings-config&gt; &gt; Network Settings &gt; Access Route</b>):</p> <ul style="list-style-type: none"> <li>• Add 0.0.0.0/0 as an access route.</li> <li>• Enter the IP address for the GlobalProtect Mobile Security Manager as an additional access route.</li> </ul>



Issue ID	Description
GPC-1517	For the GlobalProtect app to access an MDM server through a Squid proxy, you must add the MDM server SSL access ports to the proxy server allow list. For example, if the SSL access port is 8443, add <code>acl SSL_ports port 8443</code> to the allow list.
PAN-77339	The SafeNet Client 6.2.2 server does not support the necessary MAC algorithm (HMAC-SHA1) to work with Palo Alto Networks firewalls that run in FIPS-CC mode.
PAN-77237	Using the <code>debug skip-condor-reports no</code> CLI command to force Panorama 8.0 to query PA-7000 Series firewalls causes PA-7000 Series firewalls running a PAN-OS 7.0 release to reboot. Do not use this command if you use Panorama 8.0 to manage a PA-7000 Series firewall that is running a PAN-OS 7.0 release.
PAN-76162	<p>Panorama 8.0 fails to query PA-7000 Series firewalls running a PAN-OS 7.0 or PAN-OS 7.1 release.</p> <p><b>Workaround:</b> On PA-7000 Series firewalls running a PAN-OS 7.1 release, run the <code>debug skip-condor-reports no</code> command and then the <code>debug software restart process reportd</code> command to allow Panorama 8.0 to successfully query these firewalls.</p> <p> Do not use this workaround if you use Panorama 8.0 to manage a PA-7000 Series firewall that is running a PAN-OS 7.0 release (known issue <a href="#">PAN-77237</a>).</p>
PAN-75960	You cannot store the master key on an HSM in PAN-OS 8.0. Doing so will cause the firewall to enter maintenance mode after a reboot, which will require a factory reset.
PAN-75457	In WildFire appliance clusters that have three or more nodes, Panorama does not support changing node roles. For example, on Panorama, in a three-node cluster, you cannot configure the worker node as a controller node by adding the high availability and cluster controller configurations, configure an existing controller node as a worker node by removing the HA configuration, and then commit and push the configuration. Attempts to change cluster node roles from Panorama results in a validation error—the commit will fail and the cluster becomes unresponsive.
PAN-74934	Do not upgrade M-500 private cloud appliances to PAN-OS 8.0.1. Queried URLs do not resolve to a category when they are a best match to an entry in the <code>url-database</code> that has many subdomains and path levels.
PAN-73964 <i>This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a>.</i>	Do not upgrade VM-Series firewalls on AWS to PAN-OS 8.0.0 if they are deployed in a high availability (HA) configuration.
PAN-73879 <i>This issue is resolved with content release version 658 and later releases.</i>	You cannot clone the strict file blocking profile in PAN-OS 8.0; however, cloning the basic file blocking profile (or any other Security Profile types) works as expected.
PAN-73877 <i>This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a>.</i>	<p>You cannot use the firewall web interface to generate a SAML metadata file for Captive Portal or GlobalProtect if the firewall has multiple virtual systems; after you click the <b>Metadata</b> link associated with an authentication profile, no virtual systems are available to select.</p> <p><b>Workaround:</b> Access the firewall CLI, switch to the virtual system where you assigned the authentication profile (<code>set system setting target-vsyst &lt;vsyst-name&gt;</code>), and generate the metadata file (<code>show sp-metadata [captive-portal   global-protect] vsyst &lt;value&gt; authprofile &lt;value&gt; ip-hostname &lt;value&gt;</code>).</p>

Issue ID	Description
PAN-73859 This issue is now resolved. See <a href="#">PAN-OS 8.0.2 Addressed Issues</a> .	The VM-Series firewall on Azure supports only five interfaces (one management interface and four dataplane interfaces) instead of eight (one management interface and seven dataplane interfaces).
PAN-73849	After you perform a factory reset or private data reset on a fresh installation of the Panorama virtual appliance, the <b>Panorama &gt; Plugins</b> page does not display the pre-loaded VMware NSX plugin and therefore you cannot use the web interface to install the plugin. <b>Workarounds:</b> <ul style="list-style-type: none"> <li>• Use the <code>request plugins install vmware_nsx-&lt;version&gt;</code> CLI command to install the plugin.</li> <li>• Download the plugin from the Palo Alto Networks <a href="#">Support Portal</a> and then upload the plugin to Panorama. The web interface then displays the plugin for you to install.</li> </ul>
PAN-73579 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	After you upgrade a firewall to PAN-OS 8.0, the firewall does not apply updates to the predefined Palo Alto Networks malicious IP address feeds (delivered through the daily antivirus content updates) until you perform a commit on the firewall. <b>Workaround:</b> Commit changes to the firewall daily to ensure you always have the latest version of the malicious IP address feeds.
PAN-73545 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	When adding interfaces to a VM-300, VM-500, or VM-700 firewall, you must commit twice for traffic to pass normally.

Issue ID	Description
PAN-73401	<p>On a two-node WildFire appliance cluster, if you import the cluster into Panorama, the controller nodes report their state as out-of-sync if either of the following two conditions exist:</p> <ul style="list-style-type: none"> <li>You do not configure a worker list to add at least one worker node to the cluster. (In a two-node cluster, both nodes are controller nodes configured as a high-availability pair. Adding a worker node would make the cluster a three-node cluster.)</li> <li>You do not configure a service advertisement (either by enabling or not enabling advertising DNS service on the controller nodes).</li> </ul> <p><b>Workaround:</b> There are three possible workarounds to sync the controller nodes:</p> <ul style="list-style-type: none"> <li>After you import the two-node cluster into Panorama, push the configuration from Panorama to the cluster. After the push succeeds, Panorama reports that the controller nodes are in sync.</li> <li>Configure a worker list on the cluster controller:  <pre>admin@wf500(active-controller)# set deviceconfig cluster mode controller worker-list &lt;worker-ip-address&gt;</pre>           (&lt;worker-ip-address&gt; is the IP address of the worker node you are adding to the cluster.) This creates a three-node cluster. Import the cluster to Panorama and Panorama reports that the controller nodes are in sync. If you want the cluster to have only two nodes, use a different workaround.</li> <li>Configure service advertisement on the local CLI of the cluster controller and then import the configuration into Panorama. The service advertisement can advertise that DNS is enabled, or that DNS is not enabled:  <pre>admin@wf500(active-controller)# set deviceconfig cluster mode controller service-advertisement dns-service enabled yes or admin@wf500(active-controller)# set deviceconfig cluster mode controller service-advertisement dns-service enabled no</pre>           Both commands result in Panorama reporting that the controller nodes are in sync.</li> </ul>
PAN-73363 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	<p>After you enable reporting and filtering on groups, Panorama still does not display results when you filter logs or generate reports based on user groups.</p> <p><b>Workaround:</b> Access the Panorama CLI and run the <code>debug software restart process reportd operational</code> command.</p>
PAN-73316	<p>When a GlobalProtect user first logs in with a RADIUS authentication profile, the <b>Domain-UserName</b> appears as <code>user@domain</code> (instead of <code>domain\user</code>) in the PAN-OS web interface.</p> <p><b>Workaround:</b> Once a HIP report is generated, the username format is normalized and updated to the correct format.</p>
PAN-73307	<p>When you use the ACC tab to view Tunnel Activity and you <b>Jump to Logs</b>, the Tunnel Inspection logs display <code>tunnel</code> as the tunnel type.</p> <p><b>Workaround:</b> Remove tunnel type from the query in tunnel logs.</p>
PAN-73291 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	<p>If you set up client certificate authentication for GlobalProtect portals and gateways, you can specify a Certificate Profile with multiple certificate authority (CA) certificates that have the same common name. However, authentication fails for client certificates signed by a CA certificate that is not listed first in the Certificate Profile.</p>

Issue ID	Description
PAN-73254	<p>After you install the VMware NSX plugin on Panorama in a high availability (HA) deployment, Panorama does not automatically synchronize configuration changes between the HA peers unless you first update settings related to the NSX plugin.</p> <p><b>Workaround:</b> Configure the NSX settings and commit your changes to Panorama.</p>
PAN-73207 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	<p>If the firewall integrates with Okta Adaptive as the multi-factor authentication (MFA) vendor, you cannot use push notification as an authentication factor.</p>
PAN-73168	<p>If the PAN-OS web interface and the GlobalProtect portal that hosts Clientless VPN applications are configured to share the same FQDN, you can get a 400 Bad Request error from your browser when you try to access the PAN-OS web interface.</p> <p><b>Workaround:</b> Best practice is to configure separate FQDNs for the PAN-OS web interface and the GlobalProtect portal that hosts Clientless VPN applications. As a short-term fix, clear the browser cache or close all browser windows and then open a separate browser window to log in to the PAN-OS web interface.</p>
PAN-73006 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	<p>When logging rates are high, the App Scope Change Monitor and Network Monitor reports sometimes fail to display data when you filter by <b>Source</b> or <b>Destination</b> IP addresses. Additionally, the App Scope Summary report sometimes fails to display data for the Top 5 Bandwidth Consuming Source and Top 5 Threats when logging rates are high.</p>
PAN-72861	<p>When you configure a PA-5200 Series or PA-7000 Series firewall to perform tunnel-in-tunnel inspection, which includes GRE keep-alive packets (<b>Policies &gt; Tunnel Inspection &gt; Inspection &gt; Inspect Options</b>), and you run the <code>clear session all</code> CLI command while traffic is traversing a tunnel, the firewall temporarily drops tunneled packets.</p>
PAN-72843	<p>If you commit a configuration that enables clientless VPN on multiple GlobalProtect portals using different DNS proxies, the commit fails.</p> <p><b>Workaround:</b> Restart the firewall data plane and repeat the configuration commit.</p>
PAN-72402 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	<p>If you configure a BGP IPv6 aggregate address with an Advertise Filter that consists of both a prefix filter and a next-hop filter, the firewall advertises only the aggregate address and does not advertise the specific routes covered by the Advertise Filter.</p> <p><b>Workaround:</b> Remove the next-hop filter so that the firewall advertises both the aggregate address and the more specific routes. This applies only to routes learned from another BGP peer; the firewall advertises locally-injected routes as expected without this workaround.</p>
PAN-71833	<p>For a TACACS+ authentication profile, the output of the <code>test authentication authentication-profile</code> CLI command intermittently displays <code>authentication/authorization failed for user</code> even though the administrator can successfully log in to the web interface or CLI using the same credentials as were specified in the test command.</p>
PAN-71829 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	<p>In some cases, when you make specific changes on a PA-5000 Series firewall related to certificates or SSL profiles for a GlobalProtect configuration, the dataplane restarts. Changes that result in a restart include configuring a new gateway, changing a certificate linked to GlobalProtect, or changing the minimum or maximum version of the TLS profile linked to GlobalProtect; other types of changes to GlobalProtect configurations do not trigger a dataplane restart.</p>

Issue ID	Description
PAN-71765	Deactivating a VM-Series firewall from Panorama completes successfully but the web interface does not update to show that deactivation is complete. <b>Workaround:</b> View deactivation status from Managed Devices ( <b>Panorama &gt; Managed Devices</b> ).
PAN-71556 <i>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</i>	MAC address table entries with a time-to-live (TTL) value of 0 are not removed as expected in Layer 2 deployments, which results in a table that continually grows larger in size. <b>Workaround:</b> Monitor the number of table entries and run the <code>clear mac all</code> CLI command or reboot as needed to clear the table.
PAN-71334 <i>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</i>	On a PA-5200 Series firewall, when you set up a VoIP call using the Session Initiation Protocol (SIP), you can experience a delay of up to 10 seconds before the firewall transmits the audio/video stream.
PAN-71329	Local users and user groups created under Shared (all virtual systems) are not available to be part of the user-to-application mapping for GlobalProtect Clientless VPN applications ( <b>Clientless VPN &gt; Applications</b> on the GlobalProtect Portal). <b>Workaround:</b> Create users and user groups under vsys for multiple virtual systems. For single virtual systems (like VM), users and user groups are created under Shared and are not configurable for Clientless VPN applications.
PAN-71271 <i>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</i>	If the log purging process starts running before log migration begins after an upgrade to PAN-OS 8.0, the log migration process fails and drops new logs. You cannot work around this issue if the log purging process starts before you start migration. To determine whether log purging has begun, run the <code>less mp-log es_purge.log</code> CLI command, enter a forward slash ("/"), enter <code>deleting</code> , and check the output. If there are any matches, you cannot migrate; if there are no matches, then you can start log migration.
PAN-71215	Deactivating a VM-Series firewall from Panorama fails when Panorama is configured to <b>Verify Update Server Identity</b> ( <b>Panorama &gt; Setup &gt; Services &gt; Verify Update Server Identity</b> ) and this setting is disabled on the firewall ( <b>Device &gt; Setup &gt; Services</b> ); this failure causes the firewall to become unreachable. <b>Workaround:</b> Ensure that you configure both Panorama and the VM-Series firewall to <b>Verify Update Server Identity</b> before you deactivate the firewall.
PAN-70906	If the PAN-OS web interface and the GlobalProtect portal are enabled on the same IP address, then when a user logs out from the GlobalProtect portal, the administrative user is logged out from the PAN-OS web interface as well. This issue is compounded when the portal is configured for GlobalProtect Clientless VPN because it can increase the number of users who access the portal. <b>Workaround:</b> Use the IP address to access the PAN-OS web interface and an FQDN to access the GlobalProtect portal.
PAN-70353	Clientless VPN does not work if you configure the GlobalProtect portal that hosts the Clientless VPN on an interface with <b>DHCP Client</b> enabled. <b>Workaround:</b> Configure the interface to use static IP addresses.
PAN-70323 <i>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</i>	Firewalls running in FIPS-CC mode do not allow import of SHA-1 CA certificates even when the private key is not included; instead, firewalls display the following error: <code>Import of &lt;cert name&gt; failed. Unsupported digest or keys used in FIPS-CC mode.</code>

Issue ID	Description
PAN-70181	<p>PA-7000 Series firewalls that run a large number of scheduled daily reports (near 1,000 or more) will eventually experience a memory issue that causes CLI commands to fail and ultimately causes SSH connection attempts to the management IP address to fail, as well.</p> <p><b>Workaround:</b> Monitor memory usage and restart the <code>mgmtsvr</code> process when <code>mgmtsvr</code> virtual memory exceeds 6GB or <code>mgmtsvr</code> resident memory exceeds 4GB.</p>
PAN-70046	<p>A standard 404 browser error displays if you try to use GlobalProtect Clientless VPN without the correct content release version.</p> <p><b>Workaround:</b> Clientless VPN requires you to install a GlobalProtect subscription on the firewall that hosts the Clientless VPN from the GlobalProtect portal. Additionally, you need GlobalProtect Clientless VPN dynamic updates to use this feature.</p>
PAN-70027 (PLUG-216) This issue is resolved with the VMware NSX 1.0.1 plugin.	<p>The output of the <code>show object registered-IP all</code> command does not include the Source of IP tag (service profile name and ID).</p>
PAN-70023	<p>Authentication using auto-filled credentials intermittently fails when you access an application using GlobalProtect Clientless VPN.</p> <p><b>Workaround:</b> Manually enter the credentials.</p>
PAN-69874	<p>When the PAN-OS XML API sends user mappings with no timeout value to a firewall that has the <b>Enable User Identification Timeout</b> option disabled, the firewall assigns the mappings a timeout of 60 minutes instead of never.</p>
PAN-69505	<p>When viewing an external dynamic list that requires client authentication and you <b>Test Source URL</b>, the firewall fails to indicate whether it can reach the external dynamic list server and returns a URL access error.</p>
PAN-69340	<p>When you use a license authorization code (capacity license or a bundle) to bootstrap a VM-Series firewall, the capacity license is not applied. This issue occurs because the firewall does not reboot after the license is applied.</p> <p><b>Workaround:</b> Use the <code>request restart software</code> CLI command or reboot the firewall manually to activate session capacity for a VM-Series firewall.</p>
PAN-69141	<p>On PA-7000 Series firewalls and on Panorama log collectors, log collection processes consume excess memory and do not process logs as expected. This issue occurs when DNS response times are slow and scheduled reports contain fields that require DNS lookups.</p> <p><b>Workaround:</b> Use the <code>debug management-server report-namelookup disable</code> CLI command to disable DNS lookups for reporting purposes and then restart the log receiver by running <code>debug software restart process log-receiver</code>.</p>
PAN-67987 This issue is now resolved. See PAN-OS 8.0.0 Addressed Issues.	<p>The GlobalProtect agent fails to connect using a client cert if the intermediate CA is signed using the ECDSA hash algorithm.</p>
PAN-67971	<p>When you configure an endpoint running a GlobalProtect agent 3.x release to use a fully-qualified domain name (FQDN) to connect to a dual-stack PAN-OS 8.0 gateway, the firewall incorrectly displays an IPv6 address instead of an IPv4 address for the connection.</p> <p><b>Workaround:</b> Use GlobalProtect agent 4.0 to connect to PAN-OS 8.0.</p>

Issue ID	Description
PAN-67422	<p>The Firewall re-registers with WildFire every 15 days unless a connection failure occurs. If a firewall registered with a standalone WildFire appliance and then you configure the firewall to register with a WildFire appliance cluster, the firewall shows as registered both to the cluster and to the standalone appliance, which creates duplicate entries.</p> <p>To verify that a firewall is connected to a WildFire appliance and a WildFire appliance cluster, run the following command on the WildFire cluster and standalone WildFire appliance to display all firewalls registered to that cluster and appliance:</p> <pre>admin@Panorama&gt; show wildfire-appliance last-device-registration all serial-number &lt;value&gt;"</pre> <p>The &lt;value&gt; is the 12-digit serial number of the WildFire cluster controller node or the WildFire appliance. For example, to view all firewalls on a cluster whose controller node has the serial number 002001000099, run the following command:</p> <pre>admin@Panorama&gt; show wildfire-appliance last-device-registration all serial-number &lt;002001000099&gt;</pre> <p><b>Workaround:</b> Run the <code>show wildfire global devices-reporting-data</code> command to show only firewalls that are reporting data to the WildFire appliance. If a firewall has not submitted a sample to the WildFire appliance during the past 24 hours, the firewall is not listed.</p>
PAN-66122 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	Tunnel content inspection is not supported in a virtual-system-to-virtual-system topology.
PAN-66032	<p>When you monitor Block IP List entries, an IP address blocked by a Vulnerability Protection profile or Anti-Spyware profile displays the Block Source to be the Threat ID (TID) and virtual system (if applicable), instead of the name of the threat that blocked the IP address. For example, the Block Source displays 41000:vsys1 (or 41000:* if there is no virtual system).</p>
PAN-63274 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	<p>When you configure tunnel content inspection for traffic in a shared gateway topology (the firewall has multiple virtual systems), inner flow sessions installed on dataplane 1 (DP1) will fail. Additionally, when networking devices behind the shared gateway initiate traffic, that traffic doesn't reach the networking devices behind the virtual systems.</p>
PAN-62820	<p>If you use the Apple Safari browser in Private Browsing mode to request a service or application that requires multi-factor authentication (MFA), the firewall does not redirect you to the service or application even after authentication succeeds.</p>
PAN-62453	<p>Entering vSphere maintenance mode on a VM-Series firewall without first shutting down the Guest OS for the agent VMs causes the firewall to shut down abruptly and causes issues that persist after the firewall is powered on again. Refer to Issue 1332563 in the VMware release notes: <a href="https://www.vmware.com/support/pubs/nsx_pubs.html">https://www.vmware.com/support/pubs/nsx_pubs.html</a>.</p> <p><b>Workaround:</b> VM-Series firewalls are Service Virtual Machines (SVMs) pinned to ESXi hosts and should not be migrated. Before you enter vSphere maintenance mode, use the VMware tools to ensure a graceful shutdown of the VM-Series firewall.</p>
PAN-61840 This issue is now resolved. See <a href="#">PAN-OS 8.0.1 Addressed Issues</a> .	The <code>show global-protect-portal statistics</code> CLI command is not supported.



Issue ID	Description
PAN-58872	<p>The automatic license deactivation workflow for firewalls with direct internet access does not work.</p> <p><b>Workaround:</b> Use the <code>request license deactivate key features &lt;name&gt; mode manual</code> CLI command to <a href="#">Deactivate a Feature License or Subscription Using the CLI</a>. To <a href="#">Deactivate a VM</a>, choose <b>Complete Manually</b> (instead of <b>Continue</b>) and follow the steps to manually deactivate the VM.</p>
PAN-56217	<p>You cannot configure multiple DNS proxy objects that specify for the firewall to listen for DNS requests on the same interface (<b>Network &gt; DNS Proxy &gt; Interfaces</b>). If multiple DNS proxy objects are configured with the same interface, only the first DNS proxy object settings are applied.</p> <p><b>Workaround:</b> If there are DNS proxy objects configured with the same interface, you must modify the DNS proxy objects so that each object specifies unique interfaces:</p> <ul style="list-style-type: none"> <li>• To modify a DNS proxy object that specifies only one interface, delete the DNS proxy object and reconfigure the object with an interface that is not shared among any other objects.</li> <li>• To modify a DNS proxy object configured with multiple interfaces, delete the interface that is shared with other DNS proxy objects, click <b>OK</b> to save the modified object, and then <b>Commit</b>.</li> </ul>
PAN-55825	<p>Performing an AutoFocus remote search that is targeted to a PAN-OS firewall or Panorama does not work correctly when the search condition contains a single or double quotation mark.</p>
PAN-55437	<p>High availability (HA) for VM-Series firewalls does not work in AWS regions that do not support the signature version 2 signing process for EC2 API calls. Unsupported regions include AWS EU (Frankfurt) and Korea (Seoul).</p>
PAN-55203	<p>When you change the reporting period for a scheduled report, such as the SaaS Application Usage PDF report, the report can have incomplete or no data for the reporting period.</p> <p><b>Workaround:</b> If you need to change the reporting period for any scheduled report, create a new report for the desired time period instead of modifying the time period on an existing report.</p>
PAN-54254	<p>In Traffic logs, the following session end reasons for Captive Portal or a GlobalProtect SSL VPN tunnel indicated the incorrect reason for session termination: <code>decrypt-cert-validation</code>, <code>decrypt-unsupported-param</code>, or <code>decrypt-error</code>.</p>
PAN-53825	<p>For the VM-Series NSX edition firewall, when you add or modify an NSX service profile zone on Panorama, you must perform a Panorama commit and then perform a Device Group commit with the Include Device and Network Templates option selected. To successfully redirect traffic to the VM-Series NSX edition firewall, you must perform both a <b>Template</b> and a <b>Device Group</b> commit when you modify the zone configuration to ensure that the zones are available on the firewall.</p>
PAN-53663	<p>When you open the SaaS Application Usage report (<b>Monitor &gt; PDF Reports &gt; SaaS Application Usage</b>) on multiple tabs in a browser, each for a different virtual system (vsys), and you then attempt to export PDFs from each tab, only the first request is accurate; all successive attempts will result in PDFs that are duplicates of the first report.</p> <p><b>Workaround:</b> Export only one PDF at a time and wait for that export process to finish before you trigger the next export request.</p>
PAN-53601	<p>Panorama running on an M-500 appliance cannot connect to a SafeNet Network or Thales Nshield Connect hardware security module (HSM).</p>



Issue ID	Description
PAN-51969	<p>On the NSX Manager, when you unbind an NSX Security Group from an NSX Security Policy rule, the dynamic tag and registered IP address are updated on Panorama but are not sent to the VM-Series firewalls.</p> <p><b>Workaround:</b> To push the Dynamic Address Group updates to the VM-Series firewalls, you must manually synchronize the configuration with the NSX Manager (<b>Panorama &gt; VMware Service Manager</b> and select <b>NSX Config-Sync</b>).</p>
PAN-51952	<p>If a security group overlap occurs in an NSX Security policy where the same security group is weighted with a higher and a lower priority value, the traffic may be redirected to the wrong service profile (VM-Series firewall instance). This issue occurs because an NSX Security policy with a higher weight does not always take precedence over a policy with a lower weight.</p> <p><b>Workaround:</b> Make sure that members that are assigned to a security group are not overlapping with another Security group and that each security group is assigned to a unique NSX Security policy rule. This allows you to ensure that NSX Security policy does not redirect traffic to the wrong service profile (VM-Series firewall).</p>
PAN-51870	<p>When using the CLI to configure the management interface as a DHCP client, the commit fails if you do not provide all four DHCP parameters in the command. For a successful commit when using the <code>set deviceconfig system type dhcp-client</code> command, you must include each of the following parameters: <code>accept-dhcp-domain</code>, <code>accept-dhcp-hostname</code>, <code>send-client-id</code>, and <code>send-hostname</code>.</p>
PAN-51869	<p>Canceling pending commits does not immediately remove them from the commit queue. The commits remain in the queue until PAN-OS dequeues them.</p>
PAN-51673	<p>BFD sessions are not established between two RIP peers when there are no RIP advertisements.</p> <p><b>Workaround:</b> Enable RIP on another interface to provide RIP advertisements from a remote peer.</p>
PAN-51216	<p>The NSX Manager fails to redirect traffic to the VM-Series firewall when you define new Service Profile zones for NSX on Panorama. This issue occurs intermittently on the NSX Manager when you define security rules to redirect traffic to the new service profiles that are available for traffic introspection and results in the following error: <code>Firewall configuration is not in sync with NSX Manager. Conflict with Service Profile Oddhost on service (Palo Alto Networks NGFW) when binding to host&lt;name&gt;.</code></p>
PAN-51181	<p>A Palo Alto Networks firewall, M-100 appliance, or WF-500 appliance configured to use FIPS operational mode fails to boot when rebooting after an upgrade to PAN-OS 7.0 or later releases.</p> <p><b>Workaround:</b> <a href="#">Enable FIPS and Common Criteria support</a> on all Palo Alto Networks firewalls and appliances before you upgrade to a PAN-OS 7.0 or later release.</p>
PAN-51122	<p>For the VM-Series firewall, if you manually reset a heartbeat failure alarm on the vCenter server to indicate that the VM-Series firewall is healthy (change color to green), the vCenter server does not trigger a heartbeat failure alarm again.</p>

Issue ID	Description
PAN-50651	<p>On PA-7000 Series firewalls, one data port must be configured as a log card interface because the traffic and logging capabilities of this platform exceed the capabilities of the management port. A log card interface performs WildFire file-forwarding and log forwarding for syslog, email, and SNMP and these services require DNS support. If you set up a custom service route for the firewall to perform DNS queries, services using the log card interface might not be able to generate DNS requests. This is only an issue if you've configured the firewall to use a service route for DNS requests and, in this case, you must perform a workaround to enable communication between the firewall dataplane and the log card interface.</p> <p><b>Workaround:</b> Enable DNS Proxy on the firewall and do not specify an interface for the DNS proxy object to use (ensure that <b>Network &gt; DNS Proxy &gt; Interface</b> is not configured).</p>
PAN-50641	<p>Enabling or disabling BFD for BGP or changing a BFD profile that a BGP peer uses causes BGP to flap.</p>
PAN-50038	<p>When you enable jumbo frames from the CLI on a VM-Series firewall in AWS, the maximum transmission unit (MTU) size on the interfaces does not increase. The MTU on each interface remains at a maximum value of 1500 bytes.</p>
PAN-48565	<p>The VM-Series firewall on Citrix SDX does not support jumbo frames.</p>
PAN-48456	<p>IPv6-to-IPv6 Network Prefix Translation (NPTv6) is not supported when configured on a shared gateway.</p>
PAN-47969	<p>If you log in to Panorama as a Device Group and Template administrator and you rename a device group, the <b>Panorama &gt; Device Groups</b> page no longer displays any device groups.</p> <p><b>Workaround:</b> After you rename a device group, perform a commit, log out, and log back in; the page then displays the device groups with the updated values.</p>
PAN-47073	<p>Web pages using the HTTP Strict Transport Security (HSTS) protocol do not always display properly for end users.</p> <p><b>Workaround:</b> End users must import an appropriate forward-proxy-certificate for their browsers.</p>
PAN-46344	<p>When you use a Mac OS Safari browser, client certificates will not work for Captive Portal authentication.</p> <p><b>Workaround:</b> On a Mac OS system, instruct end users to use a different browser (for example, Mozilla Firefox or Google Chrome).</p>
PAN-45793	<p>On a firewall with multiple virtual systems, if you add an authentication profile to a virtual system and give the profile the same name as an authentication sequence in Shared, reference errors occur. The same errors occur if the profile is in Shared and the sequence with the same name is in a virtual system.</p> <p><b>Workaround:</b> When creating authentication profiles and sequences, always enter unique names, regardless of their location. For existing authentication profiles and sequences with similar names, rename the ones that are currently assigned to configurations (for example, a GlobalProtect gateway) to ensure uniqueness.</p>
PAN-44616	<p>On the <b>ACC &gt; Network Activity</b> tab, if you add the label Unknown as a global filter, the filter gets added as A1 and query results display A1 instead of Unknown.</p>
PAN-44400	<p>The link on a 1Gbps SFP port on a VM-Series firewall deployed on a Citrix SDX server does not come up when successive failovers are triggered. This behavior is only observed in a high availability (HA) active/active configuration.</p> <p><b>Workaround:</b> Use a 10Gbps SFP port instead of the 1Gbps SFP port on the VM-Series firewall deployed on a Citrix SDX server.</p>

Issue ID	Description
PAN-44300	WildFire analysis reports cannot be viewed on firewalls running PAN-OS 6.1 release versions if connected to a WF-500 appliance in Common Criteria mode that is running PAN-OS 7.0 or later releases.
PAN-43000	<p>Vulnerability detection of SSLv3 fails when SSL decryption is enabled. This occurs when you attach a Vulnerability Protection profile (that detects SSLv3—CVE-2014-3566) to a Security policy rule and that Security policy rule and an SSL Decryption policy rule are configured on the same virtual system in the same zone. After performing SSL decryption, the firewall sees decrypted data and no longer sees the SSL version number. In this case, the SSLv3 vulnerability is not identified.</p> <p><b>Workaround:</b> <a href="#">SSL Decryption Enhancements</a> were introduced in PAN-OS 7.0 that enable you to prohibit the inherently weaker SSL/TLS versions, which are more vulnerable to attacks. For example, you can use a Decryption Profile to enforce a minimum protocol version of TLS 1.2 or you can <b>Block sessions with unsupported versions</b> to disallow unsupported protocol versions (<b>Objects &gt; Decryption Profile &gt; SSL Decryption &gt; SSL Forward Proxy</b> and/or <b>SSL Inbound Inspection</b>).</p>
PAN-41558	<p>When you use a firewall loopback interface as a GlobalProtect gateway interface, traffic is not routed correctly for third-party IPSec clients, such as StrongSwan.</p> <p><b>Workaround:</b> Use a physical firewall interface instead of a loopback firewall interface as the GlobalProtect gateway interface for third-party IPSec clients. Alternatively, configure the loopback interface that is used as the GlobalProtect gateway to be in the same zone as the physical ingress interface for third-party IPSec traffic.</p>
PAN-40842	<p>When you configure a firewall to retrieve a WildFire signature package, the System log shows <code>unknown version</code> for the package. For example, after a scheduled WildFire package update, the system log shows: <code>WildFire package upgraded from version &lt;unknown version&gt; to 38978-45470</code>. This is a cosmetic issue only and does not prevent the WildFire package from installing.</p>
PAN-40714	<p>If you access <b>Device &gt; Log Settings</b> on a device running a PAN-OS 7.0 or later release and then use the CLI to downgrade the device to a PAN-OS 6.1 or earlier release and reboot, an error message appears the next time you access <b>Log Settings</b>. This occurs because PAN-OS 7.0 and later releases display <b>Log Settings</b> in a single page whereas PAN-OS 6.1 and earlier releases display the settings in multiple sub-pages. To clear the message, navigate to another page and return to any <b>Log Settings</b> sub-page; the error will not recur in subsequent sessions.</p>
PAN-40130	<p>In the WildFire Submissions logs, the email recipient address is not correctly mapped to a username when configuring LDAP group mappings that are pushed in a Panorama template.</p>
PAN-40079	<p>The VM-Series firewall on KVM, for all supported Linux distributions, does not support the Broadcom network adapters for PCI pass-through functionality.</p>
PAN-40075	<p>The VM-Series firewall on KVM running on Ubuntu 12.04 LTS does not support PCI pass-through functionality.</p>
PAN-39728	<p>The URL logging rate is reduced when HTTP header logging is enabled in the URL Filtering profile (<b>Objects &gt; Security Profiles &gt; URL Filtering &gt; URL Filtering profile &gt; Settings</b>).</p>

Issue ID	Description
PAN-39636	<p>Regardless of the Time Frame you specify for a scheduled custom report on a Panorama M-Series appliance, the earliest possible start date for the report data is effectively the date when you configured the report. For example, if you configure the report on the 15th of the month and set the Time Frame to Last 30 Days, the report that Panorama generates on the 16th will include only data from the 15th onward. This issue applies only to scheduled reports; on-demand reports include all data within the specified Time Frame.</p> <p><b>Workaround:</b> To generate an on-demand report, click <b>Run Now</b> when you configure the custom report.</p>
PAN-39501	<p>Unused NAT IP address pools are not cleared after a single commit, so a commit fails if the combined cache of unused pools, existing used pools, and new pools exceeds the memory limit.</p> <p><b>Workaround:</b> Commit a second time, which clears the old pool allocation.</p>
PAN-38584	<p>Configurations pushed from Panorama 6.1 and later releases to firewalls running PAN-OS 6.0.3 or earlier PAN-OS 6.0 releases will fail to commit due to an unexpected Rule Type error. This issue is caused by the <code>Rule Type</code> setting in Security policy rules that was not included in the upgrade transform and, therefore, the new rule types are not recognized on devices running PAN-OS 6.0.3 or earlier releases.</p> <p><b>Workaround:</b> Only upgrade Panorama to version 6.1 or later releases if you are also planning to upgrade all managed firewalls running PAN-OS 6.0.3 or an earlier PAN-OS 6.0 release to a PAN-OS 6.0.4 or later release before pushing a configuration to the devices.</p>
PAN-38255	<p>If you perform a factory reset on a Panorama virtual appliance and configure the serial number, logging does not work until you reboot Panorama or execute the <code>debug software restart management-server</code> CLI command.</p>
PAN-37511	<p>Due to a limitation related to the Ethernet chip driving the SFP+ ports, PA-5050 and PA-5060 firewalls will not perform link fault signaling as standardized when a fiber in the fiber pair is cut or disconnected.</p>
PAN-37177	<p>After deploying the VM-Series firewall, when the firewall connects to Panorama, you must issue a Panorama commit to ensure that Panorama recognizes the firewall as a managed device. If you reboot Panorama without committing the changes, the firewall will not connect back to Panorama; although the device group will display the list of devices, the device will not display in <b>Panorama &gt; Managed Devices</b>.</p> <p>Further, if Panorama is configured in an HA configuration, the VM-Series firewall is not added to the passive Panorama peer until the active Panorama peer synchronizes the configuration. During this time, the passive Panorama peer will log a critical message: <code>vm-cfg: failed to process registration from svm device. vm-state: active.</code> This message is logged until you commit the changes on the active Panorama, which then initiates synchronization between the Panorama HA peers and the VM-Series firewall is added to the passive Panorama peer.</p> <p><b>Workaround:</b> To reestablish the connection to the managed devices, commit your changes to Panorama (click <b>Commit</b> and select Commit Type: <b>Panorama</b>). In case of an HA setup, the commit will initiate the synchronization of the running configuration between the Panorama peers.</p>
PAN-37127	<p>On the Panorama web interface, the <b>Policies &gt; Security &gt; Post Rules &gt; Combined Rules Preview</b> window does not display post rules and local rules for managed devices.</p>
PAN-37044	<p>Live migration of the VM-Series firewall is not supported when you enable SSL decryption using the SSL forward proxy method. Use SSL inbound inspection if you need support for live migration.</p>

Issue ID	Description
PAN-36730	When deleting the VM-Series deployment, all VMs are deleted successfully; however, sometimes a few instances still remain in the datastore. <b>Workaround:</b> Manually delete the VM-Series firewalls from the datastore.
PAN-36728	In some scenarios, traffic from newly added guests or virtual machines is not steered to the VM-Series firewall even when the guests belong to a Security Group and are attached to a Security Policy that redirects traffic to the VM-Series firewall. <b>Workaround:</b> Reapply the Security Policy on the NSX Manager.
PAN-36727	The VM-Series firewall fails to deploy with an error message: <code>Invalid OVF Format in Agent Configuration</code> . <b>Workaround:</b> Use the following command to restart the ESX Agent Manager process on the vCenter Server: <code>/etc/init.d/vmware-vpxd tomcat-restart</code> .
PAN-36433	If a high availability (HA) failover occurs on Panorama at the time that the NSX Manager is deploying the VM-Series NSX edition firewall, the licensing process fails with the error: <code>vm-cfg: failed to process registration from svm device. vm-state: active</code> . <b>Workaround:</b> Delete the unlicensed instance of the VM-Series firewall on each ESXi host and then redeploy the Palo Alto Networks next-generation firewall service from the NSX Manager.
PAN-36409	When viewing the Session Browser ( <b>Monitor &gt; Session Browser</b> ), using the global refresh option (top right corner) to update the list of sessions causes the Filter menu to display incorrectly and clears any previously selected filters. <b>Workaround:</b> To maintain and apply selected filters to an updated list of sessions, click the green arrow to the right of the Filters field instead of the global (or browser) refresh option.
PAN-36394	When the datastore is migrated for a guest, all current sessions are no longer steered to the VM-Series firewall. However, all new sessions are secured properly.
PAN-36393	When deploying the VM-Series firewall, the Task Console displays <code>Error while enabling agent. Cannot complete the operation. See the event log for details</code> . This error displays even on a successful deployment. You can ignore the message if the VM-Series firewall is successfully deployed.
PAN-36333	The Service dialog for adding or editing a service object in the web interface displays the incorrect port range for both source and destination ports: <code>1-65535</code> . The correct port range is <code>0-65535</code> and specifying port number 0 for either a source or destination port is successful.
PAN-36289	If you deploy the VM-Series firewall and then assign the firewall to a template, the change is not recorded in the bootstrap file. <b>Workaround:</b> Delete the Palo Alto Networks NGFW Service on the NSX Manager, and verify that the template is specified on <b>Panorama &gt; VMware Service Manager</b> , register the service, and re-deploy the VM-Series firewall.
PAN-36088	When an ESXi host is rebooted or shut down, the functional status of the guests is not updated. Because the IP address is not updated, the dynamic tags do not accurately reflect the functional state of the guests that are unavailable.
PAN-36049	The vCenter Server/vmtools displayed the IP Address for a guest incorrectly after vlan tags were added to an Ethernet port. The display did not accurately show the IP addresses associated with the tagged Ethernet port and the untagged Ethernet port. This issue was seen on some Linux OS versions such as Ubuntu.

Issue ID	Description
PAN-35903	<p>When you edit a traffic introspection rule (to steer traffic to the VM-Series firewall) on the NSX Manager, an <code>invalid (tcp) port number error</code>—or <code>invalid (udp) port number error</code>—displays when you remove the destination (TCP or UDP) port.</p> <p><b>Workaround:</b> Delete the rule and add a new one.</p>
PAN-35875	<p>When defining traffic introspection rules (to steer traffic to the VM-Series firewall) on the NSX Manager, either the source or the destination for the rule must reference the name of a Security Group; you cannot create a rule from any to any Security Group.</p> <p><b>Workaround:</b> To redirect all traffic to the VM-Series firewall, you must create a Security Group that includes all the guests in the cluster. Then you can define a security policy that redirects traffic from and to the cluster so that the firewall can inspect and enforce policy on the east-west traffic.</p>
PAN-35874	<p>Duplicate packets are being steered to the VM-Series firewall. This issue occurs if you enable distributed vSwitch for steering in promiscuous mode.</p> <p><b>Workaround:</b> Disable promiscuous mode.</p>
PAN-34966	<p>On a VM-Series NSX edition firewall, when adding or removing a Security Group (Container) that is bound to a Security Policy, Panorama does not get a dynamic update of the added or removed Security Group.</p> <p><b>Workaround:</b> On <b>Panorama &gt; VMware Service Manager</b>, click <b>Synchronize Dynamic Objects</b> to initiate a manual synchronization to get the latest update.</p>
PAN-34855	<p>On a VM-Series NSX edition firewall, Dynamic Tags (update) do not reflect the actual IP address set on the guest. This issue occurs because the vCenter Server cannot accurately view the IP address of the guest.</p>
PAN-33316	<p>Adding or removing ports on the SDX server after deploying the VM-Series firewall can cause a configuration mismatch on the firewall. To avoid the need to reconfigure the interfaces, consider the total number of data ports that you require on the firewall and assign the relevant number of ports on the SDX server when deploying the VM-Series firewall.</p> <p>For example, if you assign ports 1/3 and 1/4 on the SDX server as data interfaces on the VM-Series firewall, the ports are mapped to eth1 and eth2. If you then add port 1/1 or 1/2 on the SDX server, eth1 will be mapped to 1/1 or 1/2, eth2 will be mapped to 1/3 and eth3 to 1/4. If ports 1/3 and 1/4 were set up as a virtual wire, this remapping will require you to reconfigure the network interfaces on the firewall.</p>
PAN-31832	<p>The following issues apply when configuring a firewall to use a hardware security module (HSM):</p> <ul style="list-style-type: none"> <li>• Thales nShield Connect—The firewall requires at least four minutes to detect that an HSM has been disconnected, causing SSL functionality to be unavailable during the delay.</li> <li>• SafeNet Network—When losing connectivity to either or both HSMs in a high availability (HA) configuration, the display of information from the <code>show ha-status</code> or <code>show hsm info</code> command is blocked for 20 seconds.</li> </ul>
PAN-31593	<p>After you configure a Panorama M-Series appliance for HA and synchronize the configuration, the Log Collector of the passive peer cannot connect to the active peer until you reboot the passive peer.</p>
PAN-29441	<p>The Panorama virtual appliance does not write summary logs for traffic and threats as expected after you enter the <code>clear log</code> command.</p> <p><b>Workaround:</b> Reboot Panorama management server (<b>Panorama &gt; Setup &gt; Operations</b>) to enable summary logs.</p>

Issue ID	Description
PAN-29411	<p>In some configurations, when you switch context from Panorama and access the web interface of a managed device, you are unable to upgrade the PAN-OS software image.  <b>Workaround:</b> Use the <b>Panorama &gt; Device Deployment &gt; Software</b> tab to deploy and install the software image on the managed device.</p>
PAN-29385	<p>You cannot configure the management IP address on an M-100 appliance while it is operating as the secondary passive peer in an HA pair.  <b>Workaround:</b> To set the IP address for the management interface, you must suspend the active Panorama peer, promote the passive peer to active state, change the configuration, and then reset the active peer to active state.</p>
PAN-29053	<p>By default, the hostname is not included in the IP header of syslog messages sent from the firewall. However, some syslog implementations require this field to be present.  <b>Workaround:</b> Enable the firewall to include the IP address of the firewall as the hostname in the syslog header by selecting <b>Send Hostname in Syslog (Device &gt; Setup)</b>.</p>
PAN-28794	<p>If a Panorama Log Collector MGT port is configured with an IPv4 address and you want to have only an IPv6 address configured, you can use the Panorama web interface to configure the new IPv6 address but you cannot use Panorama to remove the IPv4 address.  <b>Workaround:</b> Configure the MGT port with the new IPv6 address and then apply the configuration to the Log Collector and test connectivity using the IPv6 address to ensure that you do not lose access when you remove the IPv4 address. After you confirm the Log Collector is accessible using the IPv6 address, go to the CLI on the Log Collector and remove the IPv4 address (using the <code>delete deviceconfig system ip-address</code> command) and then commit your changes.</p>
PAN-25101	<p>If you add a Decryption policy rule that instructs the firewall to block SSL traffic that was not previously being blocked, the firewall will continue to forward the undecrypted traffic.  <b>Workaround:</b> Use the <code>debug dataplane reset ssl-decrypt exclude-cache</code> command to clear the SSL decrypt exclude cache.</p>
PAN-25046	<p>SSH host keys used for SCP log export are stored in the known hosts file on the firewall. In a high availability (HA) configuration, the SCP log export configuration is synchronized with the peer device, but the known host file is not synchronized. When a failover occurs, the SCP log export fails.  <b>Workaround:</b> Log in to each peer in HA and <b>Test SCP server connection</b> to confirm the host key so that SCP log forwarding continues to work after a failover.</p>
PAN-23732	<p>When you use Panorama templates to schedule a log export (<b>Device &gt; Scheduled Log Export</b>) to an SCP server, you must log in to each managed device and <b>Test SCP server connection</b> after the template is pushed. The connection is not established until the firewall accepts the host key for the SCP server.</p>
PAN-20656	<p>Attempts to reset the master key from the web interface (<b>Panorama &gt; Master Key and Diagnostics</b>) or the CLI on Panorama will fail. However, this should not cause a problem when pushing a configuration from Panorama to a device because it is not necessary for the keys to match.</p>



Issue ID	Description
PAN-20162	If a client PC uses RDP to connect to a server running remote desktop services and the user logs in to the remote server with a different username, when the User-ID agent queries the Active Directory server to gather user to IP mapping from the security logs, the second username will be retrieved. For example, if UserA logs in to a client PC and then logs in to the remote server using the username for UserB, the security log on the Active Directory server will record UserA, but will then be updated with UserB. The username UserB is then picked up by the User-ID agent for the user to IP mapping information, which is not the intended user mapping.

## Known Issues Specific to the WF-500 Appliance

The following list includes known issues specific to WildFire 8.0 releases running on the WF-500 appliance. See also the specific and general [Known Issues Related to PAN-OS 8.0 Releases](#).

Issue ID	Description
WF500-4218	As part of and after upgrading a WildFire appliance to a PAN-OS 8.0 release, rebooting a cluster node ( <code>request cluster reboot-local-node</code> ) sometimes results in the node going offline or failing to reboot. <b>Workaround:</b> Use the <code>debug cluster agent restart-agent</code> CLI command to bring the node back online and to restart the cluster agent as needed.
WF500-4200	The Create Date shown when using the <code>show wildfire global sample-status sha256 equal &lt;hash&gt;</code> and <code>show wildfire global sample-analysis</code> commands is two hours behind the actual time for WF-500 appliance samples.
WF500-4186	In a three-node WildFire appliance cluster, if you decommission the backup controller node or the worker node ( <code>request cluster decommission start</code> ) and then delete the cluster-related configuration (high-availability and cluster membership) from the decommissioned node, in some cases, the cluster stops functioning. Running the <code>show cluster membership</code> command on the primary controller node shows: Service Summary: Cluster:offline, HA:peer-offline In this state, the cluster does not function and does not accept new samples for processing. <b>Workaround:</b> Reboot the primary controller (run the <code>request cluster reboot-local-node</code> command on the primary controller's local CLI). After the primary controller reboots, the cluster functions again and accepts new samples for processing.
WF500-4176	After you remove a node from a cluster, if the cluster was storing sample information on that node, that serial number of that node may appear in the list of storage nodes when you show the sample status ( <code>show wildfire global sample-status sha256 equal &lt;value&gt;</code> ) even though the node no longer belongs to the cluster.
WF500-4173	Integrated reports are not available for firewalls connected to a WF-500 appliance running in FIPS mode.



Issue ID	Description
WF500-4166	<p>In a WildFire appliance cluster with three or more nodes and with two controller nodes, if you try to configure a worker node as a controller node, the change should fail because a cluster can have only two controller nodes (primary and backup controller nodes). However, the commit operation on the worker node succeeds and causes the cluster to see the worker node as a third controller node that cannot be allowed in the cluster. This prevents the converted worker node from connecting to the cluster manager and the node is removed from the cluster. The result when running the <code>show cluster task local</code> command displays:</p> <pre>Server error: Cannot connect to 'cluster-mgr' daemon, please check it is running. Status Report: &lt;node-ip-address&gt;: reported leader &lt;ip-address&gt;, age 0. &lt;node-ip-address&gt;: quit cluster due to too many controllers.</pre> <p><b>Workaround:</b> Perform the following tasks to workaround this issue:</p> <ol style="list-style-type: none"> <li>1. Reconfigure the node to run in worker mode using the <code>set deviceconfig cluster mode worker</code> command.</li> <li>2. Run the <code>commit force</code> command. (A standard commit operation fails and returns a message that the cluster manager is non-responsive.)</li> <li>3. After the commit force operation succeeds, reboot the node using the <code>request cluster reboot-local-node</code> command. Until you reboot the node, the node's application services do not respond.</li> </ol>
WF500-4158	<p>When you upgrade WildFire appliance clusters from Panorama, do not <b>Reboot device after Install</b>. Rebooting the cluster from Panorama results in an ungraceful reboot that causes the cluster to become unresponsive in some cases.</p> <p><b>Workaround:</b> Push the upgrade from Panorama with <b>Reboot device after Install</b> disabled. After the software upgrade is complete, reboot each cluster node individually using the <code>request cluster reboot-local-node</code> command on each node's local CLI.</p>
WF500-4132	<p>If you remove a node from a two-node WildFire appliance cluster by deleting the high-availability configuration (<code>delete deviceconfig high-availability</code>) and the cluster configuration (<code>delete deviceconfig cluster</code>), the single remaining cluster node cannot process samples.</p> <p><b>Workaround:</b> Use either of the follow workarounds to enable the remaining cluster node to process samples:</p> <ul style="list-style-type: none"> <li>• <b>Make the cluster node a standalone WildFire appliance</b>—Delete the HA and cluster configurations on the remaining cluster node and reboot the node. The node comes back up as a standalone WildFire appliance.</li> <li>• <b>Re-create the cluster</b>—Reconfigure the node you removed as a cluster node by adding the cluster and HA configurations using the following commands so that both nodes come back up as cluster nodes and can process samples:</li> </ul> <pre>admin@WF-500# set deviceconfig cluster cluster-name &lt;name&gt; interface &lt;cluster-communication-interface&gt; node controller admin@WF-500# set deviceconfig high-availability enabled yes interface hal port &lt;port&gt; peer-ip-address &lt;node-port-ip-address&gt; admin@WF-500# set deviceconfig high-availability election-option priority (primary   secondary) admin@WF-500# set deviceconfig high-availability interface hal-backup peer-ip-address &lt;node-backup-ha-interface-ip-address&gt;</pre>

Issue ID	Description
WF500-4047	<p>In a three-node WildFire appliance cluster, decommissioning the active (primary) controller node fails. Attempting to decommission the active controller node by running the <code>request cluster decommission start</code> command results in a suspension of services on the node. Use the <code>show cluster membership</code> command to verify that the node services (<code>Service Summary</code> and <code>wildfire-apps-service</code>) are suspended.</p> <p><b>Workaround:</b> Instead of using the <code>request cluster decommission start</code> command to decommission the active controller, failover the active controller so that it becomes the passive (backup) controller first and then decommission the passive controller:</p> <ol style="list-style-type: none"> <li>1. Ensure that preemption is not enabled (<code>Preemptive: no</code>) by running the <code>show high-availability state</code> command (preemption forces the active controller to resume its role as the active controller so that—after a failover, when the active controller comes back up—the active controller resumes its role as the active controller instead of becoming the passive backup controller). If preemption is enabled, disable preemption on the active controller by running the <code>set deviceconfig high-availability election-option preemptive no</code> command and then commit the configuration.</li> <li>2. Failover the active controller so that it becomes the passive (backup) controller by running the <code>request cluster reboot-local-node operational</code> command on the active controller.</li> <li>3. Wait for the former active controller to come up completely. Its new cluster role is the passive controller (as shown in the prompt).</li> <li>4. When the node is in the passive controller state, remove the HA configuration (<code>delete deviceconfig high-availability</code>) and the cluster configuration (<code>delete deviceconfig cluster</code>) and then commit the configuration.</li> <li>5. Decommission the node by running the <code>request cluster decommission start</code> command.</li> </ol>
WF500-4044	<p>Removing a node from a cluster using Panorama is not supported.</p> <p><b>Workaround:</b> <a href="#">Delete a node from a cluster using the local WildFire CLI.</a></p>
WF500-4001	<p>On Panorama, you can configure an authentication profile and <b>Add</b> groups or administrators to the <b>Allow List</b> in the profile (<b>Panorama &gt; Authentication Profile &gt; &lt;auth-profile&gt; &gt; Advanced</b>). However, WildFire appliances and appliance clusters support only the <code>all</code> value for the groups in the allow list for an authentication profile. The analogous WildFire appliance CLI command is <code>set shared authentication-profile &lt;name&gt; allow-list [all]</code>, with <code>all</code> as the only allowed parameter.</p> <p>Attempting to push and commit a configuration that specifies a group or name other than <code>all</code> in the authentication profile from Panorama to a WildFire appliance or appliance cluster is not successful. However, Panorama shows that the commit succeeded as the <code>Last Commit State</code> even though the configuration was not pushed to the WildFire appliance or appliance cluster. <code>Config Status</code> displays cluster nodes as <code>Out of Sync</code> and when you click <b>Last Commit State &gt; commit succeeded</b>, the <code>Last Push State Details</code> displays an error message.</p> <p>For example, if you <b>Add</b> a group named <code>abcd</code> to an authentication profile named <code>auth5</code> in Panorama and then attempt to push the configuration to a WildFire appliance cluster, Panorama returns the error <code>authentication-profile auth5 allow-list 'abcd' is not an allowed keyword</code>. This is because WildFire appliances and appliance clusters see the <code>allow list</code> argument as a keyword, not as a variable, and the only keyword allowed is <code>all</code>.</p>
WF500-3966	<p>The <code>request cluster join ip &lt;ip-address&gt;</code> CLI command is not functional and should not be used.</p>

Issue ID	Description
WF500-3935	WildFire appliances build and release all untested signatures to the connected firewalls every five minutes, which is the maximum time that a signature remains untested (not released to firewalls). When a WildFire appliance joins a cluster, if any untested (unreleased) signatures are on the appliance, they may be lost instead of migrating to the cluster, depending on when the last build of untested signatures occurred.
WF500-3892	The <code>request cluster reboot-all-nodes</code> CLI command is not functional and should not be used. <b>Workaround:</b> To reboot all nodes in a cluster, reboot each node individually using the <code>request cluster reboot-local-node</code> command from the node's local CLI.
WF500-3868	In a WildFire appliance cluster with two controller nodes in an HA configuration, under certain circumstances, synchronizing the controller node running configurations can cause a validation error that prevents the configuration from committing on the peer controller. When you run the <code>request high-availability sync-to-remote running-configuration</code> command on one controller node, it overwrites the candidate configuration on the peer controller and commits the new (synchronized) configuration. However, if you then change the configuration on the peer controller and commit the change, the commit fails and returns a validation error: Validation Error: template unexpected here <b>Workaround:</b> To avoid the validation error, on the controller node on which the commit failed, save the configuration to a file using the <code>save config to &lt;filename&gt; operational</code> command and then load the saved configuration using the <code>load config from &lt;filename&gt;</code> command.
WF500-1584	When using a web browser to view a WildFire Analysis Report from a firewall that is using a WF-500 appliance for file sample analysis, the report may not appear until the browser downloads the WF-500 certificate. This issue occurs after upgrading a firewall and the WF-500 appliance to a PAN-OS 6.1 or later release. <b>Workaround:</b> Browse to the IP address or hostname of the WF-500 appliance, which will temporarily download the certificate into the browser. For example, if the IP address of the WF-500 is 10.3.4.99, open a browser and enter <code>https://10.3.4.99</code> . You can then access the report from the firewall by selecting <b>Monitor &gt; WildFire Submissions</b> , clicking <b>log details</b> , and then clicking the <b>WildFire Analysis Report</b> tab.



# PAN-OS 8.0.2 Addressed Issues

The following tables lists the issues that are addressed in the PAN-OS® 8.0.2 release. For new features, associated software versions, known issues, and changes in default behavior in PAN-OS 8.0 releases, see [PAN-OS 8.0 Release Information](#).

Issue ID	Description
PAN-76517	Fixed an issue where Panorama did not automatically push the updated IP addresses of dynamic address groups from device groups to VM-Series firewalls for NSX.
PAN-76447	Fixed an issue where Panorama running PAN-OS 8.0 did not push aggregate BGP configurations in a template to firewalls running PAN-OS 7.1 or an earlier release.
PAN-76424	Fixed an issue where Security Lifecycle Review reports ( <b>Generate Stats Dump File</b> under <b>Device &gt; Support</b> ) displayed incorrect subtype values due to Threat ID changes.
PAN-76402	Fixed an issue where the firewall generated System logs of critical severity with the message <code>Could not connect to Cloud : SSL/TLS Authentication Failed</code> even though the firewall had no connection failures.
PAN-76331	Fixed an issue where, after upgrading to PAN-OS 8.0.1, a <b>Network &gt; DNS Proxy</b> object with ten or more <b>Static Entries</b> that mapped to the same IP address caused the firewall DNS daemon to restart, which prevented users from accessing applications that required DNS lookups.
PAN-76316	Fixed an issue where Panorama incorrectly calculated the number of Terminal Services (TS) agent configurations to be beyond the maximum that the managed firewalls supported and then failed to push device group configurations after you upgraded Panorama to PAN-OS 8.0.1.
PAN-76265	Fixed an issue where the firewall failed to retrieve user groups from an LDAP server because the server response did not have a page control value.
PAN-76258	Fixed an issue on PA-7000 Series and PA-5200 Series firewalls where users could not access applications and services through GlobalProtect when session distribution was set to round robin (default).
PAN-76244	Fixed an issue where firewalls were missing a GlobalProtect satellite configuration pushed from a Panorama template.
PAN-76105	Fixed an issue where you had to configure a license deactivation API key to manually deactivate licenses for VM-Series firewalls.
PAN-76104	Fixed an issue where the firewall stopped receiving IP port-to-username mappings from a Terminal Services (TS) agent if you set its <b>Host</b> field to an FQDN instead of an IP address.
PAN-76092	Fixed an issue where reports delivered through the Email Scheduler ( <b>Monitor &gt; PDF Reports &gt; Email Scheduler</b> ) displayed data totals as bytes instead of kilobytes (K), megabytes (M), or gigabytes (G), which made the totals hard to read.
PAN-76069	Fixed an issue where the firewall could not decrypt SSL connections due to a cache issue, which prevented users from accessing SSL websites.
PAN-76054	Fixed an issue where you could not delete a tunnel interface from a Panorama template ( <b>Network &gt; Interfaces &gt; Tunnel</b> ).

Issue ID	Description
PAN-76051	Fixed an issue where you could not push a Management (MGT) interface configuration from a Panorama template ( <b>Device &gt; Setup &gt; Interfaces</b> ) to firewalls unless you specified an <b>IP Address</b> for the interface.
PAN-76030	Fixed an issue on VM-Series firewalls where the dataplane restarted if jumbo frames were enabled on single root input/output virtualization (SR-IOV) interfaces.
PAN-75969	Fixed an issue where the <i>routed</i> process stopped responding after you checked the static route monitoring status through the web interface ( <b>Network &gt; Virtual Routers &gt; Routing &gt; Static Route Monitoring</b> ) or CLI ( <code>show routing path-monitor</code> ).
PAN-75914	Fixed an issue where the M-100 or M-500 appliance lost logs after upgrading from a PAN-OS 7.1 release to a PAN-OS 8.0 release.
PAN-75896	Fixed an issue where the firewall did not accept local IPv6 addresses that were longer than 31 characters when you configured IPv6 BGP peering.
PAN-75881	Fixed an issue where establishing a TCP session, then installing a content update, and then installing an Antivirus or WildFire update caused the firewall to discard, use wrong content, or fail to inspect and perform NAT for the session.
PAN-75863	Fixed an issue on HA Panorama M-100 appliances where the passive peer did not update the local VMWare NSX manager plugin after you upgraded from a PAN-OS 7.1 release to a PAN-OS 8.0 release, which caused a plugin mismatch with the active peer.
PAN-75721	Fixed an issue where you could not set the authentication profile <b>Type</b> to <b>None</b> ( <b>Device &gt; Authentication Profile</b> ) on a firewall in FIPS mode.
PAN-75684	Fixed an issue where a management server memory leak caused several tasks to fail, including commits, PAN-DB URL downloads, dynamic updates, and FQDN or External Dynamic List (EDL) refreshes.
PAN-75397	Fixed an issue where the Panorama management server restarted because the <code>configd</code> process stopped running after an upgrade.
PAN-75132	Fixed an issue where locally created certificates had duplicate serial numbers because the firewall did not check the serial numbers of existing certificates signed by the same CA when generating new certificates.
PAN-75048	Fixed an issue where the firewall used the default route (instead of the next best available route) when the eBGP next hop was unavailable, which resulted in dropped packets. Additionally with this fix, the default time-to-live (TTL) value for a single hop eBGP peer is changed to 1 (instead of 2).
PAN-74877	Fixed an issue where Panorama took a long time to push configurations from multiple device groups to firewalls.
PAN-74655	Fixed an issue on PA-7050, PA-5000 Series, and PA-3000 Series firewalls where users experienced slow network connectivity due to CPU utilization spikes in the network processing cards (NPCs) when the URL cache exceeded one million entries.
PAN-74640	Fixed an issue where VM-Series firewalls failed to create predict sessions for RTP and RTCP, which disrupted H.323-based video conferencing traffic. Additionally, fixed an issue where all firewall models dropped RTP packets because policy matching failed for RTP traffic.

Issue ID	Description
PAN-74613	Fixed an issue where the <code>show running url-cache statistics</code> CLI command did not display enough information to diagnose issues related to URL category resolution. With this fix, the error messages indicate what failed and the exact point of failure.
PAN-74575	Fixed an issue where the firewall did not release IP addresses assigned to interfaces after you changed the addressing <b>Type</b> from <b>DHCP Client</b> to <b>Static</b> .
PAN-74548	Fixed an issue where the Export Named Configuration dialog did not let you filter configuration snapshots by Name, which prevented you from selecting snapshots beyond the first 500. With this fix, you can now enter a filter string in the Name field to display any matching snapshots.
PAN-74412	Fixed an issue where, in Decryption policy rules with an <b>Action</b> set to <b>No Decrypt</b> , you could not use the web interface to set the decryption <b>Type</b> for matching traffic.
PAN-74403	Fixed an issue on Panorama where selecting the <b>Export to CSV</b> option for a custom report that required DNS lookups made the web interface unresponsive. To access the web interface, you then had to log in to the CLI and reboot Panorama or restart the management server.
PAN-74368	Fixed an issue where commits failed due to configuration memory limits on firewalls that had numerous Security policy rules that referenced many address objects. With this fix, the number of address objects that policy rules reference does not affect configuration memory.
PAN-74236	Fixed an issue where the User-ID process ( <i>userid</i> ) stopped responding when there were a lot of non-browser based requests from clients, which resulted in too many pan_errors disk writes.
PAN-74188	Fixed an issue where conflicting next-hop entries in the egress routing table caused the firewall to incorrectly route traffic that matched Policy-Based Forwarding (PBF) policy rules configured to <b>Enforce Symmetric Return</b> .
PAN-74161	Fixed an issue where firewalls configured in a virtual wire deployment where Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets were dropped.
PAN-74128	Fixed an issue where a session caused the dataplane to restart if the session was active during and after you installed a content update on the firewall and the update contained a decoder change.
PAN-73995	Fixed an issue where pushing configurations from Panorama caused firewall management interfaces that were configured through DHCP to release or renew every time instead of only when necessary.
PAN-73993	Fixed an issue where App-ID signature matching did not work on the firewall, which caused it to misidentify applications.
PAN-73914	A security-related fix was made to address OpenSSL vulnerabilities (CVE-2017-3731).
PAN-73859	Fixed an issue where the VM-Series firewall on Azure supported only five interfaces (one management interface and four dataplane interfaces) instead of eight (one management interface and seven dataplane interfaces).
PAN-73783	Fixed an issue where cookie-based authentication for the GlobalProtect gateway failed with the error <code>Invalid user name</code> .

Issue ID	Description
PAN-73710	Fixed an issue where the firewall did not commit changes to the NTP servers configuration ( <b>Device &gt; Setup &gt; Services</b> ) if the firewall connected to the servers through a service route and the management (MGT) interface was down.
PAN-73553	Fixed an issue where SSL Inbound Decryption failed when the private key was stored on a hardware security module (HSM).
PAN-73502	Fixed an issue where the firewall did not purge expired IP address-to-username mappings, which caused one of the root partitions to run out of free space.
PAN-73461	Fixed an issue where enabling encryption on the HA1 control link ( <b>Device &gt; High Availability &gt; General</b> ) and rebooting one HA firewall peer in an active/passive configuration caused split-brain to occur.
PAN-73381	Fixed an issue on firewalls with multiple virtual systems where users could not authenticate to a GlobalProtect portal or gateway that specified an authentication profile for which the Allow List referenced user groups instead of usernames.
PAN-73213	Fixed an issue where, when the GlobalProtect <b>Portal Login Page</b> was set to <b>Disable (Network &gt; GlobalProtect &gt; Portals &gt; General)</b> and the user entered <code>https://portal</code> in the browser URL field, the browser redirected to <code>https://portal/global-protect/login.esp</code> , which exposed that the firewall functioned as a GlobalProtect VPN. With this fix, the firewall now responds with a 502 Bad Gateway response and does not expose the function of the firewall.
PAN-73191	Fixed an issue where OSPF adjacency flapping occurred between the firewall and an OSPF peer due to queued OSPF hello packets.
PAN-73045	Fixed an issue where HA failover and failback events terminated sessions that started before the failover.
PAN-72871	Fixed an issue where the firewall displayed only part of the <b>URL Filtering Continue and Override</b> response page.
PAN-72769	A security-related fix was made to prevent brute-force attacks on the GlobalProtect external interface (CVE-2017-7945).
PAN-72697	Fixed an issue where, after a DoS attack ended, the firewall continued generating Threat logs and incrementing the session drop counter.
PAN-72350	Fixed an issue where high-volume SSL traffic intermittently added latency to SSL sessions.
PAN-72149	Fixed an issue where URL values did not display for the top websites in URL Filtering reports ( <b>Monitor &gt; PDF Reports &gt; Manage PDF Summary</b> ).
PAN-71627	Fixed an issue where the firewall failed to authenticate to a SafeNet hardware security module (HSM). With this fix, the firewall supports multiple SafeNet HSM client versions; you can select the version that is compatible with your SafeNet HSM server through the <code>request hsm client-version</code> CLI command.
PAN-71484	Fixed an issue where the firewall discarded long-lived SIP sessions after a content update, which disrupted SIP traffic.
PAN-71455	Fixed an issue where users could not access a secure website if the certificate authority that signed the web server certificate also signed multiple certificates with the same subject name in the Default Trusted Certificate Authorities list on the firewall.
PAN-71319	Updated PAN-OS to address NTP issues (CVE-2016-7433).



Issue ID	Description
PAN-70731	Fixed an issue where the firewall failed to authenticate to a SafeNet hardware security module (HSM) if the <b>Administrator Password</b> (under <b>Device &gt; Setup &gt; HSM</b> ) contained special characters.
PAN-70345	Fixed an issue where the M-Series appliances did not forward logs to a syslog server over TCP ports.
PAN-69882	Fixed an issue where firewalls that had multiple virtual systems and that were deployed in an HA active/active configuration dropped TCP sessions.
PAN-69874	Fixed an issue where, when the PAN-OS XML API sent IP address-to-username mappings with no timeout value to a firewall that had the <b>Enable User Identification Timeout</b> option disabled, the firewall assigned the mappings a timeout of 60 minutes instead of never.
PAN-68763	Fixed an issue where path monitoring failures did not produce enough information for troubleshooting. With this fix, PAN-OS supports additional debug commands and the tech support file (click <b>Generate Tech Support File</b> under <b>Device &gt; Support</b> ) includes additional registry values to troubleshoot path monitoring failures.
PAN-67412	Fixed an issue on HA firewalls where, when a user accessed applications over a GlobalProtect clientless VPN, the web browser became unresponsive for about 30 seconds after HA failover.
PAN-67029	Fixed an issue where the firewall stopped forwarding logs to external services (such as a syslog server) after the firewall management server restarted unexpectedly.
PAN-66997	Fixed an issue on PA-7000 Series, PA-5200 Series, and PA-5000 Series firewalls where users who accessed applications over SSL VPN or IPSec tunnels through GlobalProtect experienced one-directional traffic.
PAN-65969	Fixed an issue on PA-7000 Series firewalls where the Switch Management Card (SMC) restarted due to false positive conditions (ATA errors) detected during a disk check.
PAN-63720	Fixed an issue where <b>Monitor &gt; App Scope &gt; Network Monitor</b> displayed incorrect byte totals and hourly distribution when you filtered the report by <b>Source User/Address</b> or <b>Destination User/Address</b> instead of by <b>Application</b> .
PAN-63205	Fixed an issue on VM-Series firewalls where commit operations failed after you configured HA with the HA2 and HA3 interfaces.
PAN-62074	Fixed an issue where the User-ID agent incorrectly read the IP address in the security logs for Kerberos login events.
PAN-61409	Fixed an issue where the firewall failed to connect to an HTTP server using the HTTPS protocol when the CA certificate that validated the firewall certificate was in a specific virtual system instead of the Shared location.
PAN-60555	Fixed an issue on VM-Series firewalls for NSX where the web interface let users specify a <b>Tag Allowed</b> value for virtual wire interfaces ( <b>Network &gt; Virtual Wires</b> ), which caused a commit error because the option is not configurable on that firewall model. With this fix, the <b>Tag Allowed</b> value has a read-only value of 0-4094 on VM-Series firewalls for NSX.
PAN-55619	Fixed an issue where new users that you added to an Active Directory (AD) user group intermittently failed to authenticate to the GlobalProtect portal.
PAN-48901	Fixed an issue on HA firewalls where, if you enabled application-level gateway (ALG) for the Unistim application, VoIP calls that used the UNISTim protocol had only one-way audio after an HA failover event.

Issue ID	Description
FPGA-343	Fixed an issue on PA-7000 Series firewalls in a Layer 2 deployment where multicast sessions (such as HSRP) failed because PAN-OS did not reassign the sessions to an alternative Network Processing Card (NPC) if the original NPC was shut down.

# PAN-OS 8.0.1 Addressed Issues

The following tables lists the issues that are addressed in the PAN-OS® 8.0.1 release. For new features, associated software versions, known issues, and changes in default behavior in PAN-OS 8.0 releases, see [PAN-OS 8.0 Release Information](#).

Issue ID	Description
PAN-74932	Fixed an issue where the direction ( <i>dir</i> ) parameter used in <i>type=log</i> XML API requests was incorrectly made a required parameter, which caused applications that use the <i>type=log</i> request to fail when the <i>dir</i> argument was not included in the request. With this fix, the direction parameter is again optional.
PAN-74829	Fixed an issue where Authentication policy incorrectly matched traffic coming from known users—those included in the Terminal Services (TS) agent user mapping—and displayed the captive portal page. With this fix, only unknown users are directed to the captive portal page.
PAN-74367	Fixed an issue where some platforms did not connect to BrightCloud after you upgraded to PAN-OS 8.0.
PAN-74264	Fixed an issue where new fields in Threat and HIP Match logs were inserted between existing fields, which disrupted some third-party integrations. With this fix, the new fields are appended at the end of all pre-existing fields.
PAN-73977	Fixed an issue where firewalls and Panorama did not forward logs as expected when the local machine time was not set to current local time and was set to a time between current UTC time and current UTC time plus <i>&lt;n&gt;</i> , where <i>&lt;n&gt;</i> is the UTC+ <i>&lt;n&gt;</i> value for the current time zone.
PAN-73964	Fixed an issue where you could not upgrade <a href="#">VM-Series firewalls on AWS in an HA configuration</a> to PAN-OS 8.0. With this fix, you can upgrade VM-Series firewalls on AWS in an HA configuration to PAN-OS 8.0.1 or a later PAN-OS 8.0 release.
PAN-73877	Fixed an issue where you were unable to generate a SAML metadata file for Captive Portal or GlobalProtect when the firewall had multiple virtual systems because there were no virtual systems available for you to select when you clicked the <b>Metadata</b> link associated with an authentication profile.
PAN-73579	Fixed an issue where, after you upgraded a firewall to PAN-OS 8.0, the firewall didn't apply updates to the predefined Palo Alto Networks malicious IP address feeds (delivered through the daily antivirus content updates) until after you performed a commit on the firewall. With this fix, changes to the predefined malicious IP address feeds are automatically applied when delivered to the firewall.
PAN-73545	Fixed an issue on VM-300, VM-500, and VM-700 firewalls where you were required to commit changes a second time after adding an interface before traffic would pass normally.
PAN-73363	Fixed an issue where Panorama did not display any results when you filtered logs or generated reports based on user groups even after you enabled reporting and filtering on groups.
PAN-73360	Fixed an issue where the passive Panorama peer in an HA configuration showed shared policy to be out of sync even when the device group commit from the active peer was successful.

Issue ID	Description
PAN-73291	Fixed an issue where authentication failed for client certificates signed by a CA certificate that was not listed first in the Certificate Profile configured with client certificate authentication for GlobalProtect portals and gateways.
PAN-73207	Fixed an issue where you could not push notifications as an authentication factor if the firewall was integrated with Okta Adaptive as the multi-factor authentication (MFA) vendor.
PAN-73006	Fixed an issue where the App Scope Change Monitor and Network Monitor reports failed to display data if you filtered by <b>Source</b> or <b>Destination</b> IP addresses when logging rates were high. This fix also addresses an issue where the App Scope Summary report failed to display data for the Top 5 Bandwidth Consuming Sources and Top 5 Threats when logging rates were high.
PAN-72952	Improved file-type identification for Office Open XML (OOXML) files, which improves the ability for WildFire to accurately classify OOXML files as benign or malicious.
PAN-72849	Fixed an issue in Panorama HA active/passive configurations where Elasticsearch parameters were not pushed to the passive peer.
PAN-72726	Fixed an issue where the firewall was unable to mark BFD packets with appropriate DSCP values.
PAN-72667	Fixed an issue where the firewall web interface displayed incorrect values for the log storage quota settings.
PAN-72547	Fixed an issue where running the <code>clear session all</code> CLI command on a PA-5200 Series firewall in a high availability (HA) configuration caused the firewall to fail over due to an issue with path monitoring.
PAN-72402	Fixed an issue where the firewall advertised only the aggregate address and did not advertise the specific routes covered by the Advertise Filter when you configured a BGP IPv6 aggregate address with an Advertise Filter that consisted of both a prefix filter and a next-hop filter.
PAN-72246	Fixed an issue where the firewall generated an ECDSA certificate signing request (CSR) using the SHA1 algorithm instead of the selected algorithm.
PAN-71829	Fixed an issue on PA-5000 Series firewalls where the dataplane restarted due to specific changes related to certificates or SSL profiles in a GlobalProtect configuration; specifically, configuring a new gateway, changing a certificate linked to GlobalProtect, or changing the minimum or maximum version of the TLS profile linked to GlobalProtect.
PAN-71556	Fixed an issue where MAC address table entries with a time-to-live (TTL) value of 0 were not removed as expected, which caused the table to continually increase in size.
PAN-71530	Fixed an issue where LDAP authentication failed intermittently due to a race condition.
PAN-71334	Fixed an issue with delays of up to 10 seconds before the firewall transmitted the audio/video stream when you set up a VoIP call on a PA-5200 Series firewall using the Session Initiation Protocol (SIP).
PAN-71312	Fixed an issue where custom reports did not display results for queries that specified the <b>Negate</b> option, <b>Contains</b> operator, and a <b>Value</b> that included a period (.) character preceding a filename extension.
PAN-71271	Fixed an issue where new logs were lost if the log purging process started running before you started log migration after an upgrade to PAN-OS 8.0.

Issue ID	Description
PAN-70323	Fixed an issue where firewalls running in FIPS-CC mode did not allow import of SHA-1 CA certificates even when the private key was not included; instead, firewalls displayed the following error: Import of <cert name> failed. Unsupported digest or keys used in FIPS-CC mode.
PAN-69932	Fixed an issue where the Panorama web interface and CLI respond slowly when numerous NSX plugins are in progress.
PAN-69622	Fixed an issue where the firewall did not properly close a session after receiving a reset (RST) message from the server if the SYN Cookies action was triggered.
PAN-69585	Fixed an issue where the URL link included in the email for a SaaS Application Usage report (so that you could retrieve the report from the firewall web interface) triggered third-party spam filters deployed in your network.
PAN-68185	Fixed an issue where the 7.1 SNMP traps MIB (PAN-TRAPS.my) had an incorrect description for the <code>panHostname</code> attribute.
PAN-67629	Fixed an issue where existing users were removed from user-group mapping when the Active Directory (AD) did not return an LDAP Page Control in response to an LDAP refresh, which resulted in the following User-ID ( <i>userid</i> ) logs: <pre>debug: pan_ldap_search(pan_ldap.c:602): ldap_parse_result error code: 4 Error: pan_ldap_search(pan_ldap.c:637): Page Control NOT found</pre>
PAN-66122	Fixed an issue where tunnel content inspection was not supported in a virtual system-to-virtual system topology.
PAN-64164	Fixed an issue on Panorama virtual appliances in an HA configuration where, if you enabled log forwarding to syslog, both the active and passive peers sent logs. With this fix, only the active peer sends logs when you enable log forwarding to syslog.
PAN-63274	Fixed an issue on firewalls with multiple virtual systems where inner flow sessions installed on dataplane 1 (DP1) failed if you configured tunnel content inspection for traffic in a shared gateway topology. Additionally with this fix, when networking devices behind the shared gateway initiate traffic, that traffic can now reach the networking devices behind the virtual systems.
PAN-61840	Fixed an issue where the <code>show global-protect-portal statistics</code> CLI command was not supported.
PAN-58979	Fixed an issue where the dataplane restarted due to a memory leak ( <i>mrelay</i> ) that occurred if you did not disable LLDPDU for a disabled interface.
PAN-57553	Fixed an issue where a QoS profile failed to work as expected when applied to a clear text node configured with an Aggregate Ethernet (AE) source interface that included AE subinterfaces.
PAN-57142	Fixed an issue on PA-7000 Series firewalls in an HA active/passive configuration where QoS limits were not correctly enforced on Aggregate Ethernet (AE) subinterfaces.



# PAN-OS 8.0.0 Addressed Issues

The following tables lists the issues that are addressed in the PAN-OS® 8.0.0 release. For new features, associated software versions, known issues, and changes in default behavior in PAN-OS 8.0 releases, see [PAN-OS 8.0 Release Information](#).

Issue ID	Description
PAN-72346	Fixed an issue where exporting botnet reports failed with the following error: "Missing report job id."
PAN-72242	Fixed an issue where configuring a source address exclusion in Reconnaissance Protection tab under zone protection profile was not allowed.
PAN-71892	Fixed an issue where an LDAP profile did not use the configured port; the profile used the default port, instead.
PAN-71615	Fixed an issue where the intrazone block rule shadowed the universal rule that has different source and destination zones.
PAN-71400	Fixed an issue where the DNS Proxy feature did not work because the associated process ( <code>dnsp proxy</code> ) stopped running on a firewall that had an address object ( <b>Objects &gt; Address</b> ) with the same FQDN as one of the <b>Static Entries</b> in a DNS proxy configuration ( <b>Network &gt; DNS Proxy</b> ).
PAN-71384	Fixed an issue with the passive firewall in a high availability (HA) configuration that had LACP pre-negotiation enabled where the firewall stopped correctly processing LACP BPDU packets through an interface that had previously physically flapped.
PAN-71307	Fixed an issue where the <code>scp stats-dump</code> report did not run correctly because source ( <code>src</code> ) and destination ( <code>dst</code> ) options were determined to be invalid arguments.
PAN-71192	Fixed an issue where performing a log query or log export with a specific number of logs caused the management server to stop responding. This occurred only when the number of logs was a multiple of 64 plus 63. For example, 128 is a multiple of 64 and if you add 63 to 128 that equals 191 logs. In this case, if you performed a log query or export and there were 191 logs, the management server would stop responding.
PAN-70969	Fixed an issue on a virtual wire where, if you enabled Link State Pass Through ( <b>Network &gt; Virtual Wires</b> ), there were significant delays in link-state propagation or even instances where an interface stayed down permanently even when ports were re-enabled on the neighbor device.
PAN-70541	A security-related fix was made to address an information disclosure issue that was caused by a firewall that did not properly validate certain permissions when administrators accessed the web interface over the management (MGT) interface (CVE-2017-7644).
PAN-70483	Fixed an issue on an M-Series appliance in Panorama mode where shared service groups did not populate in the service pull down when attempting to add a new item to a security policy. The issue occurred when the drop down contained 5,000 or more entries.
PAN-70428	A security-related fix was made to prevent inappropriate information disclosure to authenticated users (CVE-2017-5583).

Issue ID	Description
PAN-70323	Fixed an issue where firewalls running in FIPS-CC mode did not allow import of SHA-1 CA certificates even when the private key was not included; instead, firewalls displayed the following error: Import of <cert name> failed. Unsupported digest or keys used in FIPS-CC mode.
PAN-70057	Fixed an issue where running the validate option on a candidate configuration in Panorama caused changes to the running configuration on the managed device. The configuration change occurred after a subsequent FQDN refresh occurred.
PAN-69951	Fixed an issue where the firewall failed to forward system logs to Panorama when the dataplane was under severe load.
PAN-69194	Fixed an issue where performing a device group commit from a Panorama server running version 7.1 to a managed firewalls running PAN-OS 6.1 failed to commit when the custom spyware profile action was set to <b>Drop</b> . With this fix, Panorama translates the action from <b>Drop</b> to <b>Drop packets</b> for firewalls running PAN-OS 6.1, which allows the device group commit to succeed.
PAN-69146	Fixed an issue where the Remote Users link for a gateway ( <b>Network &gt; GlobalProtect &gt; Gateways</b> ) became inactive and prevented you from reopening the User Information dialog if you closed the dialog using the Esc key instead of clicking <b>Close</b> .
PAN-68873	Fixed an issue where customizing the block duration for threat ID 40015 in a Vulnerability Protection profile did not adhere to the defined block interval. For example, if you set <b>Number of Hits</b> (SSH hello messages) to <b>3</b> and <b>per seconds</b> to <b>60</b> , after three consecutive SSH hello messages from the client, the firewall failed to block the client for the full 60 seconds.
PAN-68831	Fixed an issue where CSV exports for Unified logs ( <b>Monitor &gt; Logs &gt; Unified</b> ) had no log entries if you limited the effective queries to one log type.
PAN-68823	Fixed an issue where custom threat reports failed to generate data when you specified Threat Category for either the Group By or Selected Column setting.
PAN-68766	Fixed an issue where navigating to the IPSec tunnel configuration in a Panorama template caused the Panorama management web interface to stop responding and displayed a 502 Bad Gateway error.
PAN-68658	Fixed an issue where handling out-of-order TCP FIN packets resulted in dropped packets due to TCP reassembly that was out-of-sync.
PAN-68654	Fixed an issue where the firewall was not populating User-ID mappings based on the defined syslog filters.
PAN-68074	A security-related fix was made to address CVE-2016-5195.
PAN-68034	The <code>show netstat</code> CLI command was removed in the 7.1 release for Panorama, Panorama log collector, and WildFire. With this fix, the <code>show netstat</code> command is reintroduced.
PAN-67987	Fixed an issue where the GlobalProtect agent failed to connect using a client certificate if the intermediate CA is signed using the ECDSA hash algorithm.
PAN-67944	Fixed an issue where a process ( <code>all_pktproc</code> ) stopped responding because a race condition occurred when closing sessions.
PAN-67639	Fixed an issue where <code>Auth Password</code> and <code>Priv Password</code> for the SNMPv3 server profile were not properly masked when viewing the configuration change in the configuration log.



Issue ID	Description
PAN-67599	In PAN-OS 7.0 and 7.1 releases, a restriction was added to prevent an administrator from configuring OSPF router ID 0.0.0.0. This restriction is removed in PAN-OS 8.0.
PAN-67224	Fixed an issue where the firewall displayed a validation error after Panorama imported the firewall configuration and then pushed the configuration back to the firewall so it could be managed by Panorama. This issue occurred because log forwarding profiles were not replaced with the profiles configured in Panorama. With this fix, Panorama will properly remove the existing configuration on the managed firewall before applying the pushed configuration.
PAN-67090	Fixed an issue where the web interface displayed an obsolete flag for the nation of Myanmar.
PAN-67079	Fixed an issue in PAN-OS 7.1.6 where SSL sessions were discarded if the server certificate chain size exceeded 23KB.
PAN-66838	A security-related fix was made to address a Cross Site-Scripting (XSS) vulnerability on the management web interface (CVE-2017-5584).
PAN-66675	Fixed an issue where extended packet captures were consuming an excessive amount of storage space in /opt/panlogs.
PAN-66654	Fixed an issue where the status of a tunnel interface remained down even after disabling the tunnel monitoring option for IPSec tunnels.
PAN-66531	Fixed an issue where the Commit Scope column in the Commit window was empty after manually uploading and installing a content update and then committing. Although the content update was not listed under Commit Scope, the commit continued and showed 100% complete.
PAN-66104	Fixed an issue where vsys-specific custom response pages (Captive portal, URL continue, and URL override) did not display; they were replaced by shared response pages, instead.
PAN-64981	Fixed an issue where an internal buffer could be overwritten, causing the management plane to stop responding.
PAN-64870	Fixed an issue where a zone with the <b>Type</b> set to <b>Virtual Wire (Network &gt; Zones)</b> dropped all incoming traffic if the zone had a Zone Protection profile with <b>Strict IP Address Check</b> selected ( <b>Network &gt; Network Profiles &gt; Zone Protection &gt; Packet Based Attack Protection &gt; IP Drop</b> ).
PAN-64723	Fixed an issue where the <code>test authentication</code> CLI command was incorrectly sending vsys-specific information to the User-ID process for group-mapping query that allowed the authentication test to succeed when it should have failed.
PAN-64638	Fixed an issue where the firewall failed to send a RADIUS access request after changing the IP address of the management interface.
PAN-64579	Error message is now displayed when installing apps package manually from file on passive Panorama.
PAN-64525	Fixed an issue where User-ID failed to update the allow list for a group name that was larger than 128 bytes.
PAN-64520	Fixed an issue where H.323-based video calls failed when using source NAT (dynamic or static) due to incorrect translation of the <code>destCallSignalAddress</code> payload in the H.225 call setup.
PAN-64436	Fixed an issue where creation of IGMP sessions failed due to a timeout issue.

Issue ID	Description
PAN-64419	Fixed an issue where firewall displays inconsistent shadow rule warnings during a commit for QoS policies.
PAN-64081	Fixed an issue on PA-5000 Series firewalls where the dataplane stopped responding due to a race condition during hardware offload.
PAN-63969	Fixed an issue on HA PA-7050 firewalls where the transmit/receive LED for the QSFP port remained lit (indicating network activity) on the passive peer even when the link state of the port was down.
PAN-63925	Fixed an issue where the firewall did not generate a log when a content update failed or was interrupted.
PAN-63908	Fixed an issue where SSH sessions were incorrectly subjected to a URL category lookup even when SSH decryption was disabled. With this fix, SSH traffic is not subject to a URL category lookup when SSH decryption is disabled.
PAN-63612	Fixed an issue where User activity reports on Panorama did not include any entries when there was a space in the Device Group name.
PAN-63520	Fixed an issue where the wrong source zone was used when logging vsys-to-vsys sessions.
PAN-63207	Fixed an issue on PA-7000 Series firewalls where group mappings did not populate when the group include list was pushed from Panorama.
PAN-63054	Fixed an issue on VM-Series firewalls where enabling software QoS resulted in dropped packets under heavy traffic conditions. With this fix, VM-Series firewalls no longer drop packets due to heavy loads with software QoS enabled and software QoS performance in general is improved for all Palo Alto Networks firewalls.
PAN-63013	Fixed an issue where a commit validation error displayed when pushing a template configuration with a modified WildFire file-size setting. With this fix, commit validation takes place on the managed firewall that tries to commit new template values.
PAN-62937	Fixed an issue where, when TLS was enabled, establishing an LDAP connection over a slow or unstable connection caused commits to fail. With this fix, if TLS is enabled, the firewall does not attempt to establish LDAP connections when you perform a commit; it waits until after the commit is complete.
PAN-62797	Fixed an issue where a process ( <i>cdb</i> ) intermittently restarted, which prevented jobs from completing successfully.
PAN-62513	Fixed an issue on PA-7000 Series firewalls in an HA active/passive configuration where the <code>show high-availability path-monitoring</code> command always showed the NPC as <code>slot 1</code> even though the path monitoring IP address was assigned to an interface in a different NPC slot. This occurred only when the path monitoring IP address was assigned to an interface in an Aggregate Ethernet (AE) interface group and the interface group was in a slot other than slot 1.
PAN-62057	Fixed an issue where the GlobalProtect agent failed to authenticate using a client certificate that had a signature algorithm that was not SHA1/SHA256. With this fix, the firewall provides support for the SHA384 signature algorithm for client-based authentication.
PAN-61877	Fixed an issue where <b>Authentication Override</b> in the GlobalProtect portal configuration didn't work when the certificate used for encrypting and decrypting cookies was generated using RSA 4,096 bit keys.

Issue ID	Description
PAN-61871	Fixed an issue where the firewall matched traffic to a URL category and on first lookup, which caused some traffic to be matched to the wrong security profile. With this fix, the firewall matches traffic to URL categories a second time to ensure that traffic is matched to the correct security profile.
PAN-61837	Fixed an issue on PA-3000 Series and PA-5000 Series firewalls where the dataplane stopped responding when a session crossed vsys boundaries and could not find the correct egress port. This issue occurred when zone protection was enabled with a <b>SYN Cookies</b> action ( <b>Network &gt; Zone Protection &gt; Flood Protection</b> ).
PAN-61813	Fixed an issue where a custom scheduled report configured per device was empty when exported.
PAN-61797	Fixed an issue on the passive peer in an HA configuration where LACP flapped when the link state was set to shutdown/auto and pre-negotiation was disabled.
PAN-61465	Fixed an issue where the web interface ( <b>Objects &gt; Decryption Profile &gt; SSL Decryption &gt; SSL Protocol Settings &gt; Encryption Algorithms</b> ) still displayed the 3DES encryption algorithm as enabled even after you disabled it.
PAN-61365	Fixed an issue where data filtering logs ( <b>Monitor &gt; Logs &gt; Data Filtering</b> ) do not take into account the file direction (upload or download) so it was not possible to differentiate uploaded files from downloaded files in the logs. With this fix, you configure the file direction ( <b>upload, download, or both</b> ) in <b>Objects &gt; Security Profiles &gt; Data Filtering</b> and select the Direction column in <b>Monitor &gt; Logs &gt; Data Filtering</b> to view the file direction in the logs.
PAN-61284	Fixed an issue where User-ID consumed a large amount of memory when the firewall experienced a high rate of incoming IP address-to-username mapping data and there were more than ten redistribution client firewalls at the same time.
PAN-61252	Fixed an issue on firewalls in an HA active/active configuration where the floating IP address was not active on the secondary firewall after the link went down on the primary firewall.
PAN-60797	Fixed an issue where read-only superusers were able to view threat packet captures (pcaps) on the firewall but received an error ( <code>File not found</code> ) when they attempted to export certain types of pcap files (threat, threat extpcap, app, and filtering).
PAN-60753	Fixed an issue where changing the RSA key from a 2,048-bit key to a 1,024-bit key forced the encryption algorithm to change from SHA256 to SHA1 for SSL forward proxy decryption.
PAN-60581	Added check to not include all the applications in the Application filter if no application category is selected by the user. User have to explicitly add all the categories to create an application filter with all the applications.
PAN-60577	Added check in the Application Filter UI to not allow user to create or save an application filter without any application category selected by the user.
PAN-60556	Added support in the certificate profile to also configure a non CA certificate as an additional certificate to verify the OCSP response received for certificate status validation. The OCSP Verify CA field in the certificate profile has been changed to OCSP Verify Certificate.
PAN-60402	Fixed an issue where renaming an address object caused the commit to a Device Group to fail.

Issue ID	Description
PAN-60340	Fixed an issue where the Panorama application database did not display all applications in the browser.
PAN-60035	Enhanced dynamic IP NAT translation to prevent conflicts between different packet processors and improve dynamic IP NAT pool utilization.
PAN-59676	Fixed an issue where firewall administrators with custom roles (Admin Role profiles) could not download content or software updates.
PAN-59654	Fixed an issue where commits failed on the firewall after upgrading from a PAN-OS 6.1 release due to incorrect settings for the HexaTech VPN application on the firewall. With this fix, upgrading from a PAN-OS 6.1 release to a PAN-OS 8.0.0 or later release does not cause commit failures related to these settings.
PAN-59614	Fixed an issue where administrators were unable to fully utilize the maximum of 64 address objects per FQDN due to the 512B DNS server response packet size; specified addresses that were not included in the first 512B were dropped and not resolved. With this fix, the size of the DNS server response packet is increased to 4,096B, which fully supports the maximum 64 combined address objects per FQDN (up to 32 each IPv4 and IPv6 addresses).
PAN-58636	Fixed an issue where configuring too many applications and individual ports in a security rule caused the firewall to stop responding. With this fix, the firewall continues responding and sends the following error message:  <pre>Error: Security Policy '58636_rule' is exceeding maximum number of combinations supported for service ports(51) and applications(2291). To fix this, please convert this Security Policy into multiple policies by either splitting applications or service ports. Error: Failed to parse security policy (Module: device) Commit failed</pre>
PAN-58496	Fixed an issue where custom reports using threat summary were not populated.
PAN-58382	Fixed an issue where users were matched to the incorrect security policies.
PAN-57529	Fixed an issue where the firewall acted as a DHCP relay and wireless devices on a VLAN did not receive a DHCP address (all other devices on the VLAN did receive a DHCP address). With this fix, all devices on a VLAN receive a DHCP address when the firewall acts as a DHCP relay.
PAN-57440	Fixed an issue where OSPFv3 link-state updates were sent with the incorrect OSPF checksum when the OSPF packet needed to advertise more link-state advertisements (LSAs) than fit into a 1,500-byte packet. With this fix, the firewall sends the correct OSPF checksum to neighboring switches and routers even when the number of LSAs doesn't fit into a 1,500-byte packet.
PAN-57215	Fixed an issue where an HTTP 416 error appeared when trying to download updates to a client from an IBM BigFix update server.
PAN-56700	Fixed an issue where the SNMP OID ifHCOutOctets did not contain the expected data.
PAN-56684	Fixed an issue where DNS proxy static entries stopped working when there were duplicate entries in the configuration.
PAN-53659	Fixed an issue where the sum of all link aggregation group (LAG) interfaces was greater than the value of the Aggregate Ethernet (AE) interface.

## PAN-OS 8.0.0 Addressed Issues

Issue ID	Description
PAN-50973	Fixed an issue for VM-Series firewalls on Microsoft Hyper-V where, although the FIPS-CC mode option was visible in the maintenance mode menu, you could not enable it. With this fix, FIPS-CC mode is supported for and can be enabled from the maintenance mode menu in VM-Series firewalls on Microsoft Hyper-V.
PAN-48095	Fixed an issue on PA-200 firewalls where the Panorama dynamic update schedule ignored the currently installed dynamic update version and installed unnecessary dynamic updates.





# Getting Help

---

The following topics provide information on where to find more about this release and how to request support:

- ▲ [Related Documentation](#)
- ▲ [Requesting Support](#)

## Related Documentation

Refer to the following PAN-OS 8.0 documentation on the [Technical Documentation portal](#) or [search](#) the documentation for more information on our products:

- [New Features Guide](#)—Detailed information on configuring the features introduced in this release.
- [PAN-OS Administrator's Guide](#)—Provides the concepts and solutions to get the most out of your Palo Alto Networks next-generation firewalls. This includes taking you through the initial configuration and basic set up on your Palo Alto Networks firewalls.
- [Panorama Administrator's Guide](#)—Provides the basic framework to quickly set up the Panorama™ virtual appliance or an M-Series appliance for centralized administration of the Palo Alto Networks firewalls.
- [WildFire Administrator's Guide](#)—Provides steps to set up a Palo Alto Networks firewall to forward samples for WildFire™ Analysis, to deploy the WF-500 appliance to host a WildFire private or hybrid cloud, and to monitor WildFire activity.
- [VM-Series Deployment Guide](#)—Provides details on deploying and licensing the VM-Series firewall on all supported hypervisors. It includes example of supported topologies on each hypervisor.
- [GlobalProtect Administrator's Guide](#)—Describes how to set up and manage GlobalProtect™.
- [Online Help System](#)—Detailed, context-sensitive help system integrated with the firewall web interface.
- [Palo Alto Networks Compatibility Matrix](#)—Provides operating system and other compatibility information for Palo Alto Networks next-generation firewalls, appliances, and agents.
- Open Source Software (OSS) Listings—OSS licenses used with Palo Alto Networks products and software:
  - [PAN-OS 8.0](#)
  - [Panorama 8.0](#)
  - [WildFire 8.0](#)

## Requesting Support

For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to <https://www.paloaltonetworks.com/support/tabs/overview.html>.

To provide feedback on the documentation, please write to us at: [documentation@paloaltonetworks.com](mailto:documentation@paloaltonetworks.com).

## Contact Information

Corporate Headquarters:

Palo Alto Networks

4401 Great America Parkway

Santa Clara, CA 95054

<https://www.paloaltonetworks.com/company/contact-support>

Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

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

Revision Date: May 5, 2017