



TECHDOCS

PAN-OS[®] Release Notes

Version 8.0.20 (EoL)

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support.html

About the Documentation

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

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

©2017–2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

October 31, 2020

Table of Contents

PAN-OS 8.0 Release Information.....	5
Features Introduced in PAN-OS 8.0.....	6
Management Features.....	6
Panorama Features.....	8
Content Inspection Features.....	11
WildFire Features.....	13
Authentication Features.....	15
User-ID Features.....	16
App-ID Features.....	17
Decryption Features.....	18
Virtualization Features.....	19
Networking Features.....	21
GlobalProtect Features.....	25
Changes to Default Behavior.....	28
Authentication Changes.....	28
Content Inspection Changes.....	28
Decryption Changes.....	30
GlobalProtect Changes.....	30
Management Changes.....	32
Networking Changes.....	35
Panorama Changes.....	35
VM-Series Firewall Changes.....	37
WildFire Changes.....	37
CLI and XML API Changes in PAN-OS 8.0.....	38
Authentication CLI and XML API Changes.....	38
Content Inspection CLI and XML API Changes.....	39
GlobalProtect CLI and XML API Changes.....	40
Management CLI and XML API Changes.....	41
Networking CLI and XML API Changes.....	43
User-ID CLI and XML API Changes.....	44
Associated Software and Content Versions.....	46
Limitations.....	47
Known Issues.....	49
Known Issues Related to PAN-OS 8.0 Releases.....	49
Known Issues Specific to the WF-500 Appliance.....	98
PAN-OS 8.0 Addressed Issues.....	105
PAN-OS 8.0.20 Addressed Issues.....	106

PAN-OS 8.0.19-h1 Addressed Issues.....	107
PAN-OS 8.0.19 Addressed Issues.....	108
PAN-OS 8.0.18 Addressed Issues.....	109
PAN-OS 8.0.17 Addressed Issues.....	112
PAN-OS 8.0.16 Addressed Issues.....	113
PAN-OS 8.0.15 Addressed Issues.....	117
PAN-OS 8.0.14 Addressed Issues.....	121
PAN-OS 8.0.13 Addressed Issues.....	128
PAN-OS 8.0.12 Addressed Issues.....	135
PAN-OS 8.0.11-h1 Addressed Issues.....	143
PAN-OS 8.0.11 Addressed Issues.....	144
PAN-OS 8.0.10 Addressed Issues.....	151
PAN-OS 8.0.9 Addressed Issues.....	160
PAN-OS 8.0.8 Addressed Issues.....	169
PAN-OS 8.0.7 Addressed Issues.....	178
PAN-OS 8.0.6-h3 Addressed Issues.....	188
PAN-OS 8.0.6 Addressed Issues.....	189
PAN-OS 8.0.5 Addressed Issues.....	203
PAN-OS 8.0.4-h2 Addressed Issues.....	211
PAN-OS 8.0.4 Addressed Issues.....	212
PAN-OS 8.0.3-h4 Addressed Issues.....	219
PAN-OS 8.0.3 Addressed Issues.....	220
PAN-OS 8.0.2 Addressed Issues.....	228
PAN-OS 8.0.1 Addressed Issues.....	237
PAN-OS 8.0.0 Addressed Issues.....	243
Getting Help.....	253
Related Documentation.....	254
Requesting Support.....	255

PAN-OS 8.0 Release Information

Revision Date: October 28, 2019

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 PAN-OS 8.0 releases. For installation, upgrade, and downgrade instructions, refer to the [PAN-OS 8.0 New Features Guide](#).

To ensure that you are viewing the most current version of these Release Notes, always defer to the [web version](#); do not store or rely on PDF files to be current after you download them.

- > [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](#)
- > [PAN-OS 8.0.20 Addressed Issues](#)
- > [PAN-OS 8.0.19-h1 Addressed Issues](#)
- > [PAN-OS 8.0.19 Addressed Issues](#)
- > [PAN-OS 8.0.18 Addressed Issues](#)
- > [PAN-OS 8.0.17 Addressed Issues](#)
- > [PAN-OS 8.0.16 Addressed Issues](#)
- > [PAN-OS 8.0.15 Addressed Issues](#)
- > [PAN-OS 8.0.14 Addressed Issues](#)
- > [PAN-OS 8.0.13 Addressed Issues](#)
- > [PAN-OS 8.0.12 Addressed Issues](#)
- > [PAN-OS 8.0.11-h1 Addressed Issues](#)
- > [PAN-OS 8.0.11 Addressed Issues](#)
- > [PAN-OS 8.0.10 Addressed Issues](#)
- > [PAN-OS 8.0.9 Addressed Issues](#)
- > [PAN-OS 8.0.8 Addressed Issues](#)
- > [PAN-OS 8.0.7 Addressed Issues](#)
- > [PAN-OS 8.0.6-h3 Addressed Issues](#)
- > [PAN-OS 8.0.6 Addressed Issues](#)
- > [PAN-OS 8.0.5 Addressed Issues](#)
- > [PAN-OS 8.0.4-h2 Addressed Issues](#)
- > [PAN-OS 8.0.4 Addressed Issues](#)
- > [PAN-OS 8.0.3-h4 Addressed Issues](#)
- > [PAN-OS 8.0.3 Addressed Issues](#)
- > [PAN-OS 8.0.2 Addressed Issues](#)
- > [PAN-OS 8.0.1 Addressed Issues](#)
- > [PAN-OS 8.0.0 Addressed Issues](#)
- > [Related Documentation](#)
- > [Requesting Support](#)

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

PAN-OS 8.0.5 introduces support for the [Logging Service](#).

New Management Features	Description
Administrator-Level Commit and Revert	You can now commit, validate, preview, save, and revert changes that you made in a Panorama™ or firewall configuration independent of changes that other administrators have made. This simplifies your configuration workflow because you don't have to coordinate commits with other administrators when your changes are unrelated to theirs, or worry about reverting changes other administrators made that weren't ready.
NetFlow Support for PA-7000 Series Firewalls	PA-7000 Series firewalls now have the same ability as other Palo Alto Networks® firewalls to export NetFlow records 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 forward logs from PA-7000 Series firewalls to Panorama for improved log retention, which helps you meet regulatory requirements for your industry as well as your internal log archival requirements.

New Management Features	Description
Selective Log Forwarding Based on Log Attributes	<p>To enable your organization to process and respond to incident alerts more quickly, you can now create custom log forwarding filters 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.</p>
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 Selective Log Forwarding Based on Log Attributes, you can now automate security workflow more efficiently, applying dynamic policy, and responding to security incidents.</p> <ul style="list-style-type: none"> • 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 a high availability (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. • 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.
Extended SNMP Support	<p>PAN-OS support for Simple Network Management Protocol (SNMP) now includes the following features:</p> <ul style="list-style-type: none"> • 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

New Management Features	Description
	<p>individual firewalls to Panorama and external servers, and the status of firewall-to-Log Collector connections.</p> <ul style="list-style-type: none"> 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.
Increased Storage on PA-7000 Series Firewall	<p>To provide longer retention periods for logs on the PA-7000 Series firewall, you can now increase the log storage capacity 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 PA-7000 Series Firewall Log Forwarding to Panorama, which supports up to 24TB for each M-500 appliance in the Collector Group.</p>

Panorama Features

New Panorama Features	Description
Direct Query of PA-7000 Series Firewalls from Panorama (PAN-OS 8.0.8 and later releases)	<p>With the new support for PA-7000 Series Firewall Log Forwarding to Panorama, Panorama no longer treats the PA-7000 Series firewalls it manages as Log Collectors. If you have not configured your managed PA-7000 Series firewalls to forward logs to Panorama, by default you can only view the logs from the local firewall and not from Panorama. If you do not yet have a log forwarding infrastructure capable of handling the logging rate and volume from your PA-7000 Series firewalls, you can now enable Panorama to directly query managed PA-7000 Series firewalls so that you can view the logs directly from Panorama.</p>
Logging Service (PAN-OS 8.0.5 and later releases)	<p>The new Logging Service is a cloud-based service that is designed to collect and store large amounts of log data to solve your operational logging challenges. Palo Alto Networks provides the required infrastructure with scalable storage and compute that seamlessly integrates with your existing Panorama. You can continue to use your on-premise Log Collectors where they exist, or complement your logging infrastructure with this cloud-based service to which your Next-Generation Firewalls and GlobalProtect™ cloud service can directly send logs. Regardless of where the data is collected, Panorama will provide unparalleled network and threat visibility to help you prevent attacks.</p>
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</p>

New Panorama Features	Description
	<p>queries. All logs generated after the upgrade to PAN-OS 8.0 automatically take advantage of the improved query processing architecture. With this enhancement, the logging rate on the M-Series appliance is lower than in previous Panorama releases. For maximum logging rates, see Panorama Models.</p> <p>To extend the performance improvements for older logs, you can migrate the logs to the new format.</p>
<p>Logging Enhancements on the Panorama Virtual Appliance</p>	<p>You can now create a Log Collector that runs locally on the Panorama virtual appliance. Because the local Log Collector supports multiple virtual logging disks, you can increase log storage as needed while preserving existing logs. 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 Log Query Acceleration).</p>
<p>Increased Log Storage Capacity</p>	<p>To provide adequate disk space for a longer log retention period, you can increase the log storage capacity on the M-500 appliance and Panorama virtual appliance 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 Logging Enhancements on the Panorama Virtual Appliance).</p>
<p>Traps Logs on Panorama</p>	<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>
<p>Extensible Plug-in Architecture</p>	<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 VM-Series NSX Integration Configuration through Panorama. This architecture also enables support for the Cloud Services plugin, which is required for the Logging Service.</p>

New Panorama Features	Description
<p>Extended Support for Multiple Panorama Interfaces</p>	<p>To support the demands for network segmentation and security in large-scale deployments, you can now separate the management functions 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"> • 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. • 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. • 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 Streamlined Deployment of Software and Content Updates from Panorama. <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>
<p>Device Group, Template, and Template Stack Capacity Increase</p>	<p>Panorama now supports up to 1,024 Device Groups, 1,024 templates (previously 512 each), and 1,024 template stacks (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>
<p>Streamlined Deployment of Software and Content Updates from Panorama</p>	<p>You can now deploy software and content updates 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 Extended Support for Multiple Panorama Interfaces 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	<p>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 or password and block the submission.</p>
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	<p>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.</p>

New Content Inspection Features	Description
Enhanced Coverage for Command-and-Control (C2) Traffic	<p>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.</p>
GPRS Tunneling Protocol (GTP) Security (PAN-OS 8.0.4 and later releases)	<p>You can now deploy the Palo Alto Networks firewall to protect the core network in Mobile Network Operator environments that use GTP between GPRS Support Nodes (GSNs) from malformed GTP packets, denial of service attacks, out-of-state GTP messages, and protect subscribers from spoofed IP packets and over-billing attacks. Equipped with App-IDs for GTPv1-C, GTPv2-C, GTP-U, GTPv0 and GTP’, the firewall can perform stateful inspection and protocol validation on GTP control (GTPv1-C and/or GTPv2-C) and user data (GTP-U) messages, and decapsulate GTP-U packets to inspect inner IP traffic for threats and provide visibility into subscriber activity.</p> <p>The ability to statefully inspect GTP-C traffic also provides visibility into International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI), which you can correlate to the corresponding user data sessions for the subscriber. Further, for regulating subscriber access, you can filter traffic based on the IMSI/ IMSI-Prefix, Radio Access Technology (RAT), and Access Point Network (APN).</p>
Data Filtering Support for Data Loss Prevention (DLP) Solutions	<p>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.</p>
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"> • Enable Authentication for External Dynamic Lists to validate the identity of a list source and to forward login credentials for access to external dynamic lists that enforce basic HTTP authentication. • Use new Palo Alto Networks Malicious IP Address Feeds in security policy rules to block traffic from malicious IP addresses. • 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.

New Content Inspection Features	Description
New Scheduling Options for Application and Threat Content Updates	The firewall can now check for the latest App-ID, vulnerability protection, and anti-spyware signatures every 30 minutes or hourly, in addition to being able to check for these updates daily and weekly. This feature enables more immediate coverage for newly-discovered threats and strengthens safe enablement for updated and newly-defined applications.
Five-Minute Updates for PAN-DB Malware and Phishing URL Categories	The Malware and Phishing URL categories in PAN-DB are now updated every five minutes, based on the latest malicious and phishing sites the Threat Intelligence cloud 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.
Globally Unique Threat IDs	All Palo Alto Networks threat signatures now have permanent, globally unique IDs that you can use to look up threat signature information and create permanent threat exceptions: <ul style="list-style-type: none"> • 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. • Easily check if a threat signature is configured as an exception. • Use threat IDs in the Threat Vault and AutoFocus to gain context for a threat signature.
New Predefined File Blocking Profiles	Two new predefined File Blocking profiles—basic file blocking and strict file blocking—are 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.
Enhanced Unicode Decoding Support (PAN-OS 8.0.3-h4 and later releases)	The firewall can now decode UTF-16 and UTF-32 encoded data, to provide threat analysis and inspection for the encoded data.

WildFire Features



PAN-OS 8.0.1 is the base image for WF-500 appliances (not PAN-OS 8.0.0).

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 WildFire appliance clusters 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 dedicate WildFire appliance analysis resources to either documents or executables . If you are using the WildFire appliance to analyze specific file types (for example, Word documents and PDF files), 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. Verdict changes are applied only to locally-analyzed samples.
Verdict Checks with the WildFire Global Cloud	The WildFire appliance can now look up sample verdicts in the WildFire global cloud 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 WildFire Analysis of Blocked Files 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 WildFire Phishing Verdict 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.

New WildFire Features	Description
	<p>With both a WildFire license and a PAN-DB license, you can block access to phishing sites within 5 minutes of initial discovery.</p> <p>The WF-500 appliance does not support the new phishing verdict, and continues to classify suspected phishing sites as malicious.</p>

Authentication Features

New Authentication Features	Description
<p>SAML 2.0 Authentication</p>	<p>The firewall and Panorama™ can now function as Security Assertion Markup Language (SAML) 2.0 service providers to enable single sign-on (SSO) and single logout for end users (see SAML 2.0 Authentication for GlobalProtect) 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>
<p>Authentication Policy and Multi-Factor Authentication</p>	<p>To protect your network resources from attackers, you can use the new Authentication policy 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>

New Authentication Features	Description
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 use Vendor-Specific Attributes (VSAs) 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 deploy custom certificates to replace the predefined certificates shipped on Palo Alto Networks® firewalls and appliances 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>
Authentication for External Dynamic Lists	<p>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.</p>

User-ID Features

New User-ID Features	Description
Panorama and Log Collectors as User-ID Redistribution Points	<p>You can now leverage your Panorama™ and distributed log collection infrastructure to redistribute User-ID mappings in large-scale deployments. By using the existing connections from firewalls to Log</p>


New User-ID Features	Description
	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 remotely install, configure, and upgrade 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 reference more groups in policy (the limit varies by platform).
User-ID Syslog Monitoring Enhancements	<p>The following enhancements improve the accuracy of User-ID mappings and simplify monitoring syslog servers for mapping information:</p> <ul style="list-style-type: none"> • 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. • 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.
Group-Based Reporting in Panorama	Panorama now provides visibility into the activities of user groups in your network through the User Activity report, SaaS Application Usage report (see SaaS Application Visibility for User Groups), 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	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

New App-ID Features	Description
	<p>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>
<p>ALG Support for IPv6</p>	<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
<p>Decryption for Elliptical Curve Cryptography (ECC) Certificates</p>	<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> <i>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.</i></p>
<p>Management for Decryption Exclusions</p>	<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"> • A simplified workflow allows you to easily exclude traffic from decryption based on hostname. • 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

New Decryption Features	Description
	Networks predefined decryption exclusions are delivered to the firewall in content updates and are enabled by default.
Perfect Forward Secrecy (PFS) Support with SSL Inbound Inspection	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.

Virtualization Features

New Virtualization Features	Description
VM-Series Firewall Performance Enhancements and Expanded Model Line	<p>This feature introduces improved performance, capacity, and efficiency for all VM-Series firewalls, including three new VM-Series models: 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"> • 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). • 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. • 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. <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>

New Virtualization Features	Description
<p>CloudWatch Integration for the VM-Series Firewall on AWS</p>	<p>VM-Series firewalls on AWS can now natively send PAN-OS metrics to AWS CloudWatch 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 seamless license-capacity upgrades for VM-Series firewalls. 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 new Panorama™ VMware NSX plug-in 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>
<p>Support for NSX Security Tags on the VM-Series NSX Edition Firewall</p>	<p>The VM-Series firewall can now dynamically tag a guest VM with NSX securitytags 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.</p>
<p>New Serial Number Format for the VM-Series Firewall</p>	<p>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.</p>

New Virtualization Features	Description
VM-Series Bootstrapping with Block Storage	You can now bootstrap the VM-Series firewall in ESXi, KVM, and Hyper-V using block storage . 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 license deactivation API key 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 and Azure China	<p>Azure Government is a public cloud platform for U.S. government and public sector agencies. The VM-Series firewall on Azure 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).</p> <p>The VM-Series firewall is also available as a BYOL option on the Azure China marketplace.</p>
VM Monitoring on Azure	VM Monitoring of Microsoft® Azure® resources enables you to dynamically update security policy rules to consistently enforce Security policy across all assets deployed within your Azure subscription. VM Monitoring on Azure uses a VM Monitoring script that runs on a virtual machine within the Azure public cloud. This script collects the IP address-to-tag mapping for all your Azure assets and uses the API to push the VM information to your Palo Alto Networks® firewall(s).


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"> • Generic Routing Encapsulation (GRE) • Non-encrypted IPSec traffic (NULL Encryption Algorithm for IPSec and transport mode AH IPSec)

New Networking Features	Description
	<ul style="list-style-type: none"> General Packet Radio Service (GPRS) Tunneling Protocol for User Data (GTP-U) <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 tunnel content inspection 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. For information on full GTP inspection, see GPRS Tunneling Protocol (GTP) Security.</p>
Multiprotocol BGP	<p>The firewall now supports Multiprotocol BGP (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.</p> <p>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 path monitoring 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 (RDNSS) and DNS Search List (DNSSL) options, eliminating the need for a separate</p>

New Networking Features	Description
	<p>DHCPv6 server. The firewall sends IPv6 Router Advertisements with these options; thus, your IPv6 hosts are configured with:</p> <ul style="list-style-type: none"> • The addresses of RDNS servers that can resolve DNS queries. • 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.
<p>NDP Monitoring for Fast Device Location</p>	<p>You can now enable Neighbor Discovery Protocol (NDP) monitoring 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>
<p>Zone Protection for Non-IP Protocols on a Layer 2 VLAN or Virtual Wire</p>	<p>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 control non-IP protocols 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.</p>
<p>Global and Zone Protection for Multi-path TCP (MPTCP) Evasions</p>	<p>You can now enable or disable Multi-path TCP (MPTCP) globally or for each network zone. MPTCP is an extension of TCP that allows a client to simultaneously use multiple paths (instead of a single path) to connect with a destination host. MPTCP especially benefits mobile users, enabling them to maintain dual connections to both Wi-Fi and cellular networks as they move—this improves both the resilience and quality of the mobile connection and enhances the user experience. However, MPTCP can also potentially be leveraged by attackers as part of an evasion technique. This feature provides the flexibility to enable or disable MPTCP for all firewall traffic or for individual network zones, based on the visibility, performance, and security requirements for each network zone.</p>
<p>Zone Protection for SYN Data Payloads</p>	<p>You can now drop TCP SYN and SYN-ACK packets 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</p>

New Networking Features	Description
	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.
Hardware IP Address Blocking	When you configure the firewall with a DoS Protection policy or Vulnerability Protection profile to block packets 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, then IP blocking mechanisms in the software block the excess traffic. This feature is supported on PA-3050, PA-3060, PA-5000 Series, PA-5200 Series, and PA-7000 Series firewalls.
Packet Buffer Protection	Packet buffer protection 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 whitelist source addresses to exclude them from reconnaissance protection . This allows you to protect your network from reconnaissance attacks while allowing legitimate monitoring tools.
IKE Peer and IPSec Tunnel Capacity Increases	The PA-7000 Series, PA-5000 Series, and PA-3000 Series firewalls now support more IKE peers and IPSec tunnels than in prior releases. 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.
ECMP Enhancement to IP Hash	ECMP has a new load balancing option that uses an IP hash of the source address in the packet header. The Use Source Address Only option ensures that all sessions belonging to the same source IP address

New Networking Features	Description
(PAN-OS 8.0.3 and later releases)	<p>always take the same path from the available multiple paths, thus making troubleshooting easier.</p> <p> <i>If you enable the Use Source Address Only option, you shouldn't push the configuration from Panorama™ to firewalls running PAN-OS 8.0.2, 8.0.1, or 8.0.0.</i></p>

GlobalProtect Features

New GlobalProtect Features	Description
Clientless VPN	<p>You can now use Clientless VPN for securing remote access to common enterprise web applications that use HTML, HTML5, and JavaScript technologies. Users have the advantage of securing 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 (SSO) 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.</p>
IPv6 for GlobalProtect	<p>GlobalProtect clients and satellites can now connect to portals and gateways using IPv6. 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.</p>
Define Split Tunnels by Excluding Access Routes	<p>You can now exclude specific destination IP subnets traffic from being sent over the VPN tunnel. With this feature, you can send latency-sensitive or high-bandwidth-consuming traffic outside of the VPN tunnel while all other traffic is routed through the VPN for inspection and policy enforcement by the GlobalProtect gateway.</p>

New GlobalProtect Features	Description
External Gateway Priority by Source Region	GlobalProtect can now use the geographic region of the GlobalProtect client to determine the best external gateway. By including source region as part of the 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 restrict internal gateway connection choices based on the source IP address 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.
GlobalProtect Agent Login Enhancement	To simplify GlobalProtect agents and prevent unnecessary login prompts when a username and password are not required, the panel that showed portal, username, and password is now split into two screens (one screen for the portal 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 Authentication Policy and Multi-Factor Authentication enhancements within GlobalProtect 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 SAML 2.0 Authentication . If you have chosen SAML as your authentication standard, GlobalProtect portals and gateways can act as Security Assertion Markup Language (SAML) 2.0 service providers and GlobalProtect clients can authenticate users directly to the SAML identity provider.
Restrict Transparent Agent Upgrades to Internal Network Connections	You can now control when transparent upgrades occur for a GlobalProtect client. With this configuration, if the user connects from outside the corporate network, the upgrade is postponed. Later, when the user connects from within the corporate network, the upgrade is activated. This feature allows you to hold the updates until users can take advantage of good network availability and high bandwidth from

New GlobalProtect Features	Description
	<p>within the corporate network. The upgrades will not hinder users when they travel to environments with low bandwidth.</p>
<p>AirWatch MDM Integration</p>	<p>The PAN-OS Windows User-ID agent has been extended to support a new AirWatch MDM Integration 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.</p>
<p>Increased Capacity for Split Tunnel Include Access Routes (PAN-OS 8.0.2 and later releases)</p>	<p>The firewall now supports up to 800 access routes used to include traffic in a split tunnel gateway configuration on Chromebooks and up to 1000 access routes on all other endpoints. 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 the PAN-OS 8.0 New Features Guide.</p>


Changes to Default Behavior

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

- [Authentication Changes](#)
- [Content Inspection Changes](#)
- [Decryption Changes](#)
- [GlobalProtect Changes](#)
- [Management Changes](#)
- [Networking 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	 <i>(PAN-OS 8.0.2 and later releases)</i> 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	The defaults for the following TCP Settings (Device > Setup > Session > TCP Settings) is changed in 8.0:

Feature	Change
	<ul style="list-style-type: none"> • Drop segments without flag 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. • Drop segments with null timestamp option 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. • Forward segments exceeding TCP out-of-order queue is now disabled by default. The corresponding CLI command, <code>set deviceconfig setting tcp bypass-exceed-oo-queue</code> is now set to <code>no</code> by default.
Content-ID™	<p>Forward segments exceeding TCP App-ID inspection queue (Device > Setup > Content-ID > Content-ID Settings) 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 Objects > Decryption Profile, edit the profile, select SSL Decryption > SSL Forward Proxy, and in the Unsupported Mode Checks section select Block sessions with unsupported cipher suites. To skip decryption for such connections, clear Block sessions with unsupported cipher suites.</p>
URL Filtering	<p>When a firewall running PAN-OS 8.0 connects with PAN-DB (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>Objects > Custom Objects > Data Patterns provides predefined patterns (Pattern Type > Predefined Pattern), 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>

Feature	Change
Application filters	You must now select at least one Category when creating or modifying an application filter (Objects > Application Filters). This optimizes firewall performance when filtering applications, as the firewall includes only the categories that are relevant to you.
DoS Protection and Vulnerability 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.

Decryption Changes

PAN-OS® 8.0 has the following change in default behavior for decryption:

Feature	Change
Perfect Forward Secrecy (PFS) Support with SSL Inbound Inspection	<p>Beginning in PAN-OS 8.0, firewalls use the Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE) algorithm to perform strict certificate checking. This means that if the firewall uses an intermediate certificate, you must re-import the certificate from your web server to the firewall after you upgrade to a PAN-OS 8.0 or later release and combine the server certificate with the intermediate certificate (install a chained certificate); otherwise, SSL Inbound Inspection sessions that use an intermediate certificate will fail.</p> <p>Use the following procedure to install a chained certificate:</p> <ol style="list-style-type: none"> 1. Open each certificate (.cer) file in a plain-text editor. 2. Paste each certificate end-to-end with the Server Certificate at the top with each signer included below. 3. Save the file as a text (.txt) or certificate (.cer) file (the name of the file cannot contain blank spaces). 4. Import the combined (chained) certificate in to the firewall.

GlobalProtect Changes

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

Feature	Change
GlobalProtect portals and gateways	<ul style="list-style-type: none"> • The Agent > Gateways tab for GlobalProtect portal configurations is split into two separate tabs: Internal and External. Use the Internal tab to specify internal gateway settings for GlobalProtect agents and apps. Use the External tab to specify external gateway settings


Feature	Change						
	<p>for GlobalProtect agents and apps. These are layout changes only—your existing PAN-OS 7.1 configuration is preserved.</p> <ul style="list-style-type: none"> • The Agent > Client Settings > Network Settings tab for GlobalProtect gateway configurations is replaced with two separate tabs: IP Pools and Split Tunnel. These are layout changes only—your existing PAN-OS 7.1 configuration is preserved. • The selectable Disable login page option on the General tab for GlobalProtect portal configurations is now a Disable command in the Portal Login Page. This is a layout change only—your existing PAN-OS 7.1 configuration is preserved. • (PAN-OS 8.0.5 and later releases) To improve access control for GlobalProtect portals and gateways (internal or external), even when user endpoints have valid authentication override cookies, PAN-OS now matches the users against the Allow List of authentication profiles (Device > Authentication Profile > <authentication_profile> > Advanced). Modifying the Allow List is an easy way to prevent unauthorized access by users who have valid cookies but disabled accounts. 						
IP address pools	<p>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.</p>						
Clientless VPN	<p>The option to Allow user to launch unpublished applications is now renamed Display application URL address bar. The new option name better reflects the purpose of this option.</p>						
Web interfaces changes	<p>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.</p>						
	<table border="1"> <thead> <tr> <th data-bbox="529 1577 846 1650">Location</th> <th data-bbox="846 1577 1159 1650">PAN-OS 7.1 Label</th> <th data-bbox="1159 1577 1471 1650">PAN-OS 8.0 Label</th> </tr> </thead> <tbody> <tr> <td data-bbox="529 1650 846 1787">The General tab for GlobalProtect portal configurations</td> <td data-bbox="846 1650 1159 1787">Custom Login Page</td> <td data-bbox="1159 1650 1471 1787">Portal Login Page</td> </tr> </tbody> </table>	Location	PAN-OS 7.1 Label	PAN-OS 8.0 Label	The General tab for GlobalProtect portal configurations	Custom Login Page	Portal Login Page
	Location	PAN-OS 7.1 Label	PAN-OS 8.0 Label				
The General tab for GlobalProtect portal configurations	Custom Login Page	Portal Login Page					

Feature	Change		
	The General tab for GlobalProtect portal configurations	Custom Help Page	App Help Page
	The Agent > External > Add > External Gateway 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
Log Forwarding	(PAN-OS 8.0.6 and later releases) Connections to a Syslog server over TLS are validated using the Online Certificate Status Protocol (OCSP) when available. However, you cannot bypass OCSP failures so you must ensure the certificate chain is valid and can be verified using OCSP.
PA-7000 Series Log Collection	<p>After you upgrade to PAN-OS 8.0, Panorama will no longer consider the PA-7000 Series firewall as a Log Collector; all logs the firewall generates after upgrade will be viewable only from the local firewall and not from Panorama.</p> <p>After you upgrade your Panorama appliance to PAN-OS 8.0.8 (or a later release), you can configure Panorama to directly query PA-7000 Series firewalls when you select Remote Device Data as the Data Source by running the following command from the Panorama CLI:</p> <pre>> debug-reportd send-request-to-7k yes</pre> <p>This only enables Panorama to query the PA-7000 Series firewalls it manages. To run reports on PA-7000 Series log data, you must enable log forwarding to Panorama on each PA-7000 Series firewall that Panorama manages.</p> <p>This means that, after you upgrade you must enable log forwarding to Panorama if you want to continue to see an aggregated view of your logs from Panorama.</p>

Feature	Change
	<p> Before you upgrade your PA-7000 Series firewall to PAN-OS 8.0, make sure your Log Collectors have enough capacity to support the log collection rates required by your PA-7000 Series firewall. Refer to the Table: Panorama Log Storage and Collection Rates (Panorama Models) to determine if your existing logging infrastructure can handle the logging rate and log storage requirements of your PA-7000 Series firewalls. If you are not sure of the logging rate, run the following CLI command from the firewall:</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>> debug log-receiver statistics</p> </div> <p>As soon as you enable log forwarding to Panorama, the PA-7000 Series firewall begins forwarding new logs to Panorama. However, to maintain the ability to view historic log data on Panorama, you need to migrate the logs from the PA-7000 Series firewall to the Log Collector.</p>
Management access	<ul style="list-style-type: none"> • 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 configure an SSL/TLS service profile that allows TLSv1.0 and assign the profile to the interface used to access the firewall or Panorama. • To configure the management (MGT) interface on the firewall, you now select Device > Setup > Interfaces instead of Device > Setup > Management.
Configuration backups	<p>To create a snapshot file for the candidate configuration, you must now select Config > Save Changes instead of Save at the top right of the web interface.</p>
External dynamic lists	<ul style="list-style-type: none"> • 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. • 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. • Entries in an external dynamic list (IP addresses, domains, and URLs) now only count toward the maximum number that the firewall

Feature	Change
	<p>supports if a security policy rule references the external dynamic list.</p>
<p>Anti-Spyware profiles</p>	<p>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.</p>
<p>Service routes</p>	<p>The firewall now uses the new service route Palo Alto Networks Services to access external services that it accessed via the service routes Palo Alto Updates and WildFire Public prior to PAN-OS 8.0.</p>
<p>Content and software updates</p>	<ul style="list-style-type: none"> Beginning with PAN-OS 8.0, the Verify Update Server Identity global services setting for installing content and software updates is enabled by default (Device > Setup > Services > Global). PAN-OS now evaluates the last five content release versions instead of just the newest version when checking the Palo Alto Networks Update Server for a version that matches the Threshold age configured in an update schedule on a firewall (Device > Dynamic Updates > <update_type_schedule>) or a Panorama management server (Panorama > Dynamic Updates > <update_type_schedule>). This change ensures that an update is available for PAN-OS to perform the Action configured in an update schedule (download-only or download-and-install) when the Threshold age exceeds the frequency at which Palo Alto Networks releases the updates. For example, if a firewall has a Threshold of 48 hours for Applications and Threats content updates but Palo Alto Networks releases the updates every 24 hours, the latest update will never reach the 48-hour age Threshold required to trigger the Action, but one of the four previous updates will. PAN-OS checks the last five content release versions for Antivirus updates also.
<p>Log Forwarding</p>	<ul style="list-style-type: none"> Firewalls, Panorama management servers, and Dedicated Log Collectors now support only TLSv1.2 for the SSL/TLS connections used to forward logs to syslog servers. (PAN-OS 8.0.6 and later releases) Firewalls, Panorama management servers, and Dedicated Log Collectors now check the revocation status of syslog server certificates as an enhancement to improve security when connecting to syslog servers.

Feature	Change
Logging for RAID events	M-Series appliances, PA-7000 Series firewalls, and PA-5200 Series firewalls now generate System logs with a severity level set to critical instead of medium for the <code>disk-failed</code> , <code>disk-faulty</code> , and <code>pair-disappeared</code> RAID events.

Networking Changes

PAN-OS 8.0 has the following changes in default behavior.

Feature	Change
BGP	The BGP peer connection settings include Multi Hop, which is the TTL value in the IP header. The default value of 0 means 2 for eBGP prior to PAN-OS 8.0.2, and it means 1 beginning with PAN-OS 8.0.2.
First packet broadcasting	(PAN-OS 8.0.1 and later 8.0 releases) The option to broadcast the first packet for a session to all the dataplanes on a firewall is now disabled by default on PA-5000 Series firewalls: the first packet goes only to the first dataplane (DP0). Enabling first packet broadcasting improves firewall performance during session setup. However, the dataplanes become unstable when you enable both first packet broadcasting and jumbo frames. To enable or disable first packet broadcasting, use the set session broadcast-first-packet [no yes] CLI command.

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 Panorama > Setup > Interfaces (instead of Panorama > Setup > Management).
Log collection	<ul style="list-style-type: none"> When adding or editing a Log Collector (Panorama > Managed Collectors), you now configure interfaces in the Interfaces tab, which replaces the Management, Eth1, and Eth2 tabs in the Collector dialog.

Feature	Change
	<ul style="list-style-type: none"> • 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. • Logs databases have been consolidated on both M-Series appliances in Panorama mode and Dedicated Log Collectors. <ul style="list-style-type: none"> • Detailed Firewall Logs—Traffic, Threat, Application Statistics, URL, Wildfire® Submissions, Data Filtering, HIP Match, User-ID™, Tunnel, and Authentication • Summary Firewall Logs—Traffic Summary, Threat Summary, URL Summary, and Tunnel Inspection Summary • Infrastructure and Audit Logs—Config, System, and User-ID • Palo Alto Networks® Platform Logs—Traps™ ESM and Aperture™ • Third-Party External Logs • By default, 4% of the total disk space has been allocated for the newly introduced Palo Alto Networks Platform Logs and 3rd Party External Logs and databases.
Commit and push operations	<ul style="list-style-type: none"> • 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. • With these commit workflow changes on Panorama that allow you to choose whether to commit on Panorama, push to devices, or commit and push, Commit is available (green) even when you have no pending changes on Panorama and all managed firewalls and Log Collectors are in sync with Panorama (which means that you have successfully pushed all changes you made on Panorama to all managed firewalls and appliances).
Content and software updates	<p>Firewalls and Log Collectors now retrieve software and content updates from Panorama over port 28443 instead of Panorama pushing the updates over port 3978.</p>
NAT deployment	<p>(PAN-OS 8.0.8 and later releases) To enable a Panorama management server that is behind a NAT device and that runs a PAN-OS 8.0 or later release to manage firewalls that are also running PAN-OS 8.0 or a later release, you must run a new CLI command in operational mode on Panorama: set dlsrvr server [FQDN IP-address], where [FQDN IP-address] is the IP address or FQDN of the Panorama management (MGT) interface. To display the current value of this setting, run the show dlsrvr server command. If you stop</p>

Feature	Change
	deploying a NAT device between Panorama and firewalls, delete the value by running the delete dlsrvr server command.

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 is 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 Virtualization Features .
Large Receive Offload	Large Receive Offload (LRO) is enabled by default on new deployments of the VM-Series firewall for NSX and on deployments upgraded to PAN-OS 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"> If you previously enabled WildFire forwarding on your firewall, in addition to forwarding unknown files for WildFire analysis, the firewall now forwards blocked files that match existing signatures. Additionally, the WildFire Submissions log now includes log entries for blocked files. The Action column in the WildFire Submissions log now indicates if the firewall action for a sample was allow or block. In PAN-OS 7.1 and earlier versions, the action displayed for all samples in the WildFire Submissions log was alert.

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 character (">") while configuration commands are preceded by a hash character ("#"). An asterisk ("*") indicates that related commands in the same hierarchy have also changed.

- [Authentication CLI and XML API Changes](#)
- [Content Inspection CLI and XML API Changes](#)
- [GlobalProtect CLI and XML API Changes](#)
- [Management CLI and XML API Changes](#)
- [Networking CLI and XML API Changes](#)
- [User-ID CLI and XML API Changes](#)

Authentication CLI and XML API 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"> • PAN-OS 7.1 and earlier releases: <pre>> show running captive-portal-policy > test cp-policy-match * # show rulebase captive-portal * # set import resource max-cp-rules <0-4000> # set rulebase captive-portal * # set shared admin-role <name> role device webu i policies captive-portal-rulebase {enable read-only d isable} # set import resource max-cp-rules <0-4000></pre> • PAN-OS 8.0 release: <pre>> show running authentication-policy > test authentication-policy-match * # show rulebase authentication * # set import resource max-auth-rules <0-4000> # set rulebase authentication rules * # set shared admin-role <name> role device webu i policies</pre>

Feature	Change
	<pre>authentication-rulebase {enable read-only disable} # set import resource max-auth-rules <0-4000></pre>
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"> • PAN-OS 7.1 and earlier releases: <pre># set deviceconfig setting ssl-decrypt fwd-proxy-server-cert-key-size {0 1024 2048}</pre> <ul style="list-style-type: none"> • PAN-OS 8.0 release: <pre># set deviceconfig setting ssl-decrypt fwd-proxy-server-cert-key-size-rsa {0 1024 2048} # set deviceconfig setting ssl-decrypt fwd-proxy-server-cert-key-size-ecdsa {0 256 384}</pre>
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"> • PAN-OS 7.1 and earlier releases: <pre># show deviceconfig system hsm-settings provider safenet-luna-sa * # set deviceconfig system hsm-settings provider safenet-luna-sa *</pre> <ul style="list-style-type: none"> • PAN-OS 8.0 release: <pre># show deviceconfig system hsm-settings provider safenet-network * # set deviceconfig system hsm-settings provider safenet-network *</pre>

Content Inspection CLI and XML API 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"> • PAN-OS 7.1 and earlier releases: <pre># set external-list <name> *</pre> • PAN-OS 8.0 release: <pre># set external-list <name> type ip * # set external-list <name> type predefined-ip * # set external-list <name> type domain * # set external-list <name> type url *</pre>
Applications and threats	<p>(PAN-OS 8.0.4 and later releases) The XML API call for retrieving detailed information on applications and threats from the firewall has changed:</p> <ul style="list-style-type: none"> • PAN-OS 8.0.3 and earlier releases: <pre>https://<firewall>/api/? type=config&action=get&xpath=/config/ predefined/threats</pre> • PAN-OS 8.0.4 and later releases: <pre>https://<firewall>/api/? type=op&cmd=<show>predefined<xpath>/predefined/ threats </xpath>/predefined</show></pre>

GlobalProtect CLI and XML API 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"> • PAN-OS 7.1 and earlier releases: <pre># set global-protect global-protect-portal <name> portal-config local-address ip <value></pre>

Feature	Change
	<ul style="list-style-type: none"> <li data-bbox="597 226 899 258">• PAN-OS 8.0 release: <pre data-bbox="646 300 1430 491"># set global-protect global-protect-portal <name> portal-config local-address ip ipv4 <value> # set global-protect global-protect-portal <name> portal-config local-address ip ipv6 <value></pre> <li data-bbox="597 527 1057 558">• PAN-OS 7.1 and earlier releases: <pre data-bbox="646 600 1430 699"># set global-protect global-protect-portal <name> portal-config local-address floating-ip <value></pre> <li data-bbox="597 735 899 766">• PAN-OS 8.0 release: <pre data-bbox="646 808 1430 999"># set global-protect global-protect-portal <name> portal-config local-address floating-ip ipv4 <value> # set global-protect global-protect-portal <name> portal-config local-address floating-ip ipv6 <value></pre>

Management CLI and XML API Changes

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

Feature	Change
Log retention on Log Collectors	<p data-bbox="597 1350 1430 1449">(PAN-OS 8.0.2 and later releases) The operational command to determine the effective log retention periods on Log Collectors is changed.</p> <p data-bbox="597 1491 1349 1797"> <i>In certain cases, the effective retention period for each log type differs from its configured retention period (Panorama > Collector Groups > <Collector_Group> > General > Log Storage). This happens when the amount of used storage approaches the maximum quota for a log type, forcing the Log Collector to delete the oldest logs of that type even if those logs don't exceed the configured retention period. The Log Collector deletes old logs to clear space for new logs.</i></p>

Feature	Change
	<ul style="list-style-type: none"> • PAN-OS 8.0.1 and earlier releases: <pre data-bbox="634 296 1456 352">> show system logdb-quota</pre> • PAN-OS 8.0.2 and later releases: <ul style="list-style-type: none"> • On Dedicated Log Collectors, the command is: <pre data-bbox="672 491 1456 548">> show log-collector-es-indices</pre> • On the Panorama management server (local Log Collectors), the command for each Collector Group is: <pre data-bbox="672 680 1456 762">> show log-collector-es-indices log-collector-grp-name <CG_name></pre> <p data-bbox="634 785 1435 1094">You can determine the effective retention periods by checking the dates of the Oldest indices in the command output. Each index has the following format: pan_<year><month><day>_<log_type>, where <year><month><day> indicates the date of the index. In the following example, the oldest Configuration and System logs (cfigsys) are dated February 2, 2017 (20170202) and the oldest Traffic Summary logs (trsum) are dated February 14, 2017 (20170214):</p> <pre data-bbox="634 1136 1456 1255">Oldest indices: pan_20170202_cfigsys_0007se00004 pan_20170214_trsum_0007se00004</pre>
Log forwarding	<p data-bbox="597 1297 1456 1394">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"> • PAN-OS 7.1 and earlier releases: <pre data-bbox="634 1493 1456 1791"># 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 <name> * # set shared log-settings profiles <name> *</pre>

Feature	Change
	<ul style="list-style-type: none"> • PAN-OS 8.0 release: <pre data-bbox="634 296 1455 814"> # 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 <name> match-list * # set shared log-settings profiles <name> match-list *</pre>

Networking CLI and XML API Changes

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

Feature	Change
BGP Minimum Route Advertisement Interval (MRAI)	<p>(PAN-OS 8.0.11 and later PAN-OS 8.0 releases only) A new operational command introduced to manually make a global change to the BGP MRAI timer (range is 1 to 600; default is 30):</p> <ul style="list-style-type: none"> • PAN-OS 8.0.11 and later PAN-OS 8.0 releases: <pre data-bbox="583 1339 1455 1430"> > set system setting bgp-mrai-timer value <seconds></pre>
Network connections and statistics	<p>The operational command to display network connections and statistics has changed:</p> <ul style="list-style-type: none"> • PAN-OS 7.1 and earlier releases: <pre data-bbox="583 1625 1455 1688"> > request netstat statistics *</pre> • PAN-OS 8.0 and later releases: <pre data-bbox="583 1772 1455 1835"> > show netstat statistics *</pre>

User-ID CLI and XML API 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"> 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"> PAN-OS 7.1 and earlier releases: <pre data-bbox="623 543 1455 606">> clear user-cache {all ip}</pre> PAN-OS 8.0 release: <pre data-bbox="623 690 1455 753">> clear ipuser-cache {all ip}</pre> The User-ID commands to clear user mappings from the dataplane have changed: <ul style="list-style-type: none"> PAN-OS 7.1 and earlier releases: <pre data-bbox="623 926 1455 1010">> clear uid-gids-cache uid <1-2147483647> > clear uid-gids-cache all</pre> PAN-OS 8.0 release: <pre data-bbox="623 1100 1455 1184">> clear uid-cache uid <1-2147483647> > clear uid-cache all</pre>
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"> PAN-OS 7.1 and earlier releases: <pre data-bbox="584 1388 1455 1692"># set user-id-agent <name> host {<ip/netmask> <value>} # set user-id-agent <name> port <1-65535> # set user-id-agent <name> ntlm-auth {yes no} # set user-id-agent <name> ldap-proxy {yes no} } # set user-id-agent <name> collectorname <value> > # set user-id-agent <name> secret <value></pre> PAN-OS 8.0 release: <pre data-bbox="584 1787 1455 1854"># set user-id-agent <name> host-port host {<ip/netmask> <value>}</pre>

Feature	Change
	<pre> # set user-id-agent <name> host-port port <1-65535> # set user-id-agent <name> host-port ntlm-auth {yes no} # set user-id-agent <name> host-port ldap-proxy {yes no} # set user-id-agent <name> host-port collectorname <value> # set user-id-agent <name> host-port secret <value> </pre>

Associated Software and Content Versions



The following minimum software versions are compatible with PAN-OS® 8.0. To confirm which versions are currently supported, please refer to the [End-of-Life \(EoL\) summary](#).

To see a list of the Palo Alto Networks® firewalls and appliances that support PAN-OS 8.0, see the [Palo Alto Networks CompatibilityMatrix](#).

Palo Alto Networks Software or Content Release Version	Minimum Compatible Version with PAN-OS 8.0
Panorama™	8.0.2
WF-500 Appliance	8.0.1
User-ID™ Agent	8.0.0
Terminal Services (TS) Agent	8.0.0
GlobalProtect™ Agent	4.0.0
Applications and Threats Content Release Version	655
Antivirus Content Release Version	2137

Limitations

The following table includes limitations associated with PAN-OS® 8.0 releases.

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 (Panorama > Managed Wildfire Clusters) to check the cluster membership list and ensure that all listed members are nodes in the cluster and to 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 a local configuration, the Panorama web interface displays it as a standalone appliance and shows it to be out of sync. To resolve this, 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> <ul style="list-style-type: none"> <li data-bbox="537 1184 1328 1457">  <i>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.</i> <li data-bbox="537 1499 1344 1633">  <i>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 Commit to Panorama to avoid unintended consequences.</i> <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>

Issue ID	Description
	<ul style="list-style-type: none">• If you have not committed the configuration on Panorama, remove the node from the cluster.• If you have already committed the changes on Panorama, remove the node from the cluster and re-commit the changes to Panorama.• 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. <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">• If you have not committed the configuration on Panorama, specify a valid cluster node as the controller or controller backup node.• If you have already committed the changes on Panorama, specify a valid cluster node as the controller or controller backup node and Commit to Panorama.• 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.

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 to 60 minutes to complete. Ensure uninterrupted power to your firewall throughout the upgrade process.
—	A Panorama™ management server running PAN-OS 8.0 does not currently support management of appliances running WildFire® 7.1 or earlier releases. Even though these management options are visible on the Panorama 8.0 web interface (Panorama > Managed WildFire Clusters and Panorama > Managed WildFire Appliances), making changes to these settings for appliances running WildFire 7.1 or an earlier release has no effect.
GPC-2742	<p>When you configure GlobalProtect portals and gateways to use client certificates and LDAP as two factors of authentication, Chromebook users who run Chrome OS 47 or a later version can encounter excessive prompts to select a client certificate.</p> <p>Workaround: 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"> 1. Log in to the Google Admin console (https://admin.google.com) and select Device management > Chrome management > User settings. 2. In the Client Certificates section, enter the following URL pattern to Automatically Select Client Certificate for These Sites: <pre data-bbox="570 1818 1456 1877">{"pattern": "https://[*.*]", "filter": {}}</pre>

Issue ID	Description
	<p>3. Save your changes. The Google Admin console deploys the policy to all devices within a few minutes.</p>
GPC-1737	<p>By default, the GlobalProtect app adds a route on iOS mobile endpoints that causes traffic to the GP-100 GlobalProtect Mobile Security Manager to bypass the VPN tunnel.</p> <p>Workaround: 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 (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Client Settings > <client-settings-config> > Network Settings > Access Route):</p> <ul style="list-style-type: none"> • Add 0.0.0.0/0 as an access route. • Enter the IP address for the GlobalProtect Mobile Security Manager as an additional access route.
GPC-1517	<p>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 acl SSL_ports port 8443 to the allow list.</p>
PLUG-380	<p>When you rename a device group, template, or template stack in Panorama that is part of a VMware NSX service definition, the new name is not reflected in NSX Manager. Therefore, any ESXi hosts that you add to a vSphere cluster are not added to the correct device group, template, or template stack and your Security policy is not pushed to VM-Series firewalls that you deploy after you rename those objects. There is no impact to existing VM-Series firewalls.</p>
PAN-130069	<p>There is an issue where the firewall incorrectly interprets an external dynamic list MineMeld instability error code as an empty external dynamic list.</p>
PAN-126921	<p>(PA-7000 Series firewalls only) There is an issue where internal path monitoring fails when the firewall processes corrupt packets.</p>
PAN-124956	<p>There is an issue where VM-Series firewalls do not support packet buffer protection.</p>
PAN-120440	<p>There is an issue on M-500 Panorama management servers where any Ethernet interface with an IPv6 address having Private PAN-DB-URL connectivity only supports the following format: 2001:DB9:85A3:0:0:8A2E:370:2.</p>

Issue ID	Description
<p>PAN-120303</p>	<p>There is an issue where the firewall remains connected to the PAN-DB-URL server through the old management IP address on the M-500 Panorama management server, even when you configured the Eth1/1 interface.</p> <p>Workaround: Update the PAN-DB-URL IP address on the firewall using one of the methods below.</p> <ul style="list-style-type: none"> • Modify the PAN-DB Server IP address on the managed firewall. <ol style="list-style-type: none"> 1. On the web interface, delete the PAN-DB Server IP address (Device > Setup > Content ID > URL Filtering settings). 2. Commit your changes. 3. Add the new M-500 Eth1/1 IP PAN-DB IP address. 4. Commit your changes. • Restart the firewall (<i>devsvr</i>) process. <ol style="list-style-type: none"> 1. Log in to the firewall CLI. 2. Restart the devsvr process: debug software restart process device-server
<p>PAN-114041</p>	<p>(Panorama™ M-Series and virtual appliances only) There is a rare issue where, as a result of known issue PAN-107636, new Elasticsearch (ES) indices are empty, which prevents the web interface from displaying logs for the days associated with those indices.</p> <p> <i>The root cause of this issue is resolved in PAN-OS 8.1.7.</i></p>
<p>PAN-111866</p> <p>This issue is now resolved. See PAN-OS 8.0.16 Addressed Issues.</p>	<p>The push scope selection on the Panorama web interface displays incorrectly even though the commit scope displays as expected. This issue occurs when one administrator makes configuration changes to separate device groups or templates that affect multiple firewalls and a different administrator attempts to push those changes.</p> <p>Workaround: Perform one of the following tasks.</p> <ul style="list-style-type: none"> • Initiate a Commit to Panorama operation followed by a Push to Devices operation for the modified device group and template configurations. • Manually select the devices that belong to the modified device group and template configurations.
<p>PAN-111729</p>	<p>If you disable DPDK mode and enable it again, you must reboot the firewall immediately.</p>

Issue ID	Description
<p>PAN-109594</p> <p>This issue is now resolved. See PAN-OS 8.0.16 Addressed Issues.</p>	<p>(HA configurations only) The dataplane restarts when an IPsec rekey event occurs and causes a tunnel process (<i>tund</i>) failure when one—but not both—HA peers is running PAN-OS 8.0.14 or PAN-OS 8.1.5.</p> <p>Workaround: Temporarily modify the IKE phase 2 lifetime for both peers (Network > Network Profiles > IPsec Crypto) to increase the interval between rekey events (default is one hour) to avoid a rekey event before you complete the upgrade on the second peer. Alternatively, remove the HA configuration, upgrade both firewalls, and then restore the HA configuration.</p>
<p>PAN-108165</p> <p>This issue is now resolved. See PAN-OS 8.0.18 Addressed Issues.</p>	<p>Memory issues on Palo Alto Networks hardware and virtual appliances cause intermittent management plane instability.</p>
<p>PAN-107636</p> <p>This issue is now resolved. See PAN-OS 8.0.16 Addressed Issues.</p>	<p>(Panorama M-Series and virtual appliances only) There is a rare issue where the purge script does not remove the oldest Elasticsearch (ES) indices to make room for new ones as expected when the appliance reaches maximum capacity. This prevents the web interface from displaying any logs for the days associated with those new ES indices (see known issue PAN-114041) because those indices are empty (the appliances cannot read or write to them). If you experience this issue, contact your Support team for assistance.</p>
<p>PAN-106989</p>	<p>(PAN-OS 8.0.14 and later PAN-OS 8.0 releases) There is a display-only issue on Panorama that results in a <code>commit failed</code> status for Template Last Commit State (Panorama > Managed Devices > Summary).</p> <p>Workaround: Push templates to managed devices.</p>
<p>PAN-104986</p>	<p>(PA-800 Series firewalls only) Firewalls intermittently stop responding and require you to manually reboot due to an issue related to the stall detection feature.</p>
<p>PAN-103008</p>	<p>If your Panorama is managing firewalls that are running a PAN-OS 8.0 release, that are sending logs to Cortex Data Lake, and on which you enabled Secure Client Communication, the firewall cannot successfully establish TLS communication with Cortex Data Lake unless you use the default certificates.</p> <p>Workaround: Disable Secure Client Communication (Device > Setup > Management) for managed firewalls that are running a PAN-OS 8.0 release or upgrade the managed firewalls to PAN-OS 8.1 so that you can choose custom (non-default) certificates for communicating with Cortex Data Lake (firewall to Log Collector communication).</p>

Issue ID	Description
<p>PAN-102140</p> <p>This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.</p>	<p>Extended Authentication (X-Auth) clients intermittently fail to establish an IPSec tunnel to GlobalProtect gateways.</p>
<p>PAN-100244</p> <p>This issue is now resolved. See PAN-OS 8.0.14 Addressed Issues.</p>	<p>There is a rare issue where a failed commit or commit validation followed by a non-user-committed event (such as an FQDN refresh, an external dynamic list refresh, or an antivirus update) results in an unexpected change to the configuration that causes the firewall to drop traffic.</p> <p>Workaround: Perform a successful commit immediately after you experience this issue. Alternatively, reload an earlier successfully-committed configuration and manually refresh the FQDN list.</p>
<p>PAN-100154</p>	<p>(PAN-OS 8.0.12 and later PAN-OS 8.0 releases only) The default static route always becomes the active route and takes precedence over a DHCP auto-created default route that is pointing to the same gateway regardless of the metrics or order of installation. Thus, when the system has both a DHCP auto-created default route and a manually configured default static route pointing to the same gateway, the firewall always installs the default static route in the FIB.</p> <p>Workaround: Set the Default Route Metric in the web interface DHCP Client configuration (Network > Interfaces > {Ethernet VLAN} > <interface> > IPv4).</p>
<p>PAN-99483</p>	<p>(PA-5250 and PA-5260 firewalls only) When you deploy the firewall in a network that uses Dynamic IP and Port (DIPP) NAT translation with PPTP, client systems are limited to using a translated IP address-and-port pair for only one connection. This issue occurs because the PPTP protocol uses a TCP signaling (control) protocol that exchanges data using Generic Routing Encapsulation (GRE) version 1 and the hardware cannot correlate the call-id in the GRE version 1 header with the correct dataplane (the one that owns the predict session of GRE).</p> <p>Workaround: Use the set session distribution-policy symmetric-hash operational CLI command to send the GRE packet to the dataplane that owns the predict session.</p>
<p>PAN-99084</p>	<p>(HA configurations running PAN-OS 8.0.9 or a later PAN-OS 8.0 release) If you disable the high availability (HA) configuration sync option (enabled by default), User-ID data is not synced as expected between HA peers.</p> <p>Workaround: Re-Enable Config Sync (Device > High Availability > General > Setup settings).</p>

Issue ID	Description
<p>PAN-97757</p>	<p>GlobalProtect authentication fails with an Invalid username/ password error (because the user is not found in Allow List) after you enable GlobalProtect authentication cookies and add a RADIUS group to the Allow List of the authentication profile used to authenticate to GlobalProtect.</p> <p>Workaround: Disable GlobalProtect authentication cookies. Alternatively, disable (clear) Retrieve user group from RADIUS in the authentication profile and configure group mapping from Active Directory (AD) through LDAP.</p>
<p>PAN-97561</p> <p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.</p>	<p>Panorama appliances running PAN-OS 8.1.2 cannot connect to the Logging Service:</p> <ul style="list-style-type: none"> • When you deploy a Panorama 8.1.2 virtual appliance, Panorama is unable to connect to the Logging Service and firewalls are unable to forward logs to the Logging Service. • If you upgrade a Panorama virtual appliance with Logging Service enabled to PAN-OS 8.1.2, both Panorama and the firewalls will continue to connect to the Logging Service but will not display information about Logging Services instances when you run the requestlogging-service-forwarding customerinfo fetch CLI command.
<p>PAN-97524</p>	<p>(Panorama management server only) The Security Zone and Virtual System columns (Network tab) display None after a Device Group and Template administrator with read-only privileges performs a context switch.</p>
<p>PAN-96734</p> <p>This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.</p>	<p>The configuration daemon (<i>configd</i>) stops responding during a partial revert operation when reverting an interface configuration.</p>
<p>PAN-96587</p> <p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.</p>	<p>PA-7000 Series and PA-5200 Series firewalls intermittently fail to forward logs to Log Collectors or the Logging Service due to DNS resolution failure for the FQDNs of those log receivers.</p> <p>Workaround: On the firewall, commit a configuration change or run the debug software restart process log-receiver CLI command.</p>
<p>PAN-96572</p> <p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.</p>	<p>After end users successfully authenticate for access to a service or application, their web browsers briefly display a page indicating that authentication completed and then they are redirected to an unknown URL that the user did not specify.</p>

Issue ID	Description
PAN-OS 8.0.12 Addressed Issues.	
PAN-96158	<p>(PAN-OS 8.0.11 and later PAN-OS 8.0 releases) After an HA firewall cluster with graceful restart enabled on routing protocols fails over, it does not immediately display the connected, static, and host routes as Active. This issue does not impact performance and the routes typically display as Active, again, within 30 seconds after the failover.</p>
PAN-96113 This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues.	<p>In a deployment where the firewall connects to a Border Gateway Protocol (BGP) peer that advertises a route for which the next hop is not in the same subnetwork as the BGP peer interface, the show routing protocol bgp rib-out CLI command does not display advertised routes that the firewall sent to the BGP peer.</p> <p>Workaround: Move the next hop to the same subnetwork as the BGP peer interface.</p>
PAN-95999 This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues.	<p>Firewalls in an HA active/active configuration with a default session setup and owner configuration drop packets in a GlobalProtect VPN tunnel that uses a floating IP address.</p>
PAN-95773	<p>On VM-Series firewalls that have Data Plane Development Kit (DPDK) enabled and that use the i40e network interface card (NIC), the show session info CLI command displays an inaccurate throughput and packet rate.</p> <p>Workaround: Disable DPDK by running the set system setting dpdk-pkt-io off CLI command.</p>
PAN-95736 This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.	<p>The <i>mprelay</i> process stops responding when a commit occurs while the firewall is identifying flows that need a NetFlow update.</p>
PAN-95717	<p>After 30,000 or more end users log in to the GlobalProtect gateway within a two- to three-hour period, the firewall web interface responds slowly, commits take longer than expected or intermittently fail, and Tech Support File generation times out and fails.</p>
PAN-95534	<p>(PAN-OS 8.0.6 and later releases) The firewall does not provide an option to disable revocation status checks for syslog server certificates, and therefore log forwarding to syslog servers fails when the TLS certificate chains are not properly set up. Only firewalls running PAN-</p>

Issue ID	Description
	<p>OS 8.0.6 and later releases check the revocation status of syslog server certificates.</p> <p>Workaround: Ensure the syslog servers send the full TLS certificate chains.</p>
PAN-95511	<p>The name for an address object, address group, or an external dynamic list must be unique. Duplicate names for these objects can result in unexpected behavior when you reference the object in a policy rule.</p>
<p>PAN-95445</p> <p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues; fix requires the VMware NSX 2.0.4 or later plugin.</p>	<p>VM-Series firewalls for NSX and firewalls in an NSX notify group (Panorama > VMware NSX > Notify Group) briefly drop traffic while receiving dynamic address updates after the primary Panorama in an HA configuration fails over.</p>
<p>PAN-95197</p> <p>This issue is now resolved. See PAN-OS 8.0.10 Addressed Issues.</p>	<p>Mobile endpoints that use GPRS Tunneling Protocol (GTP) lose traffic and have to reconnect because the firewall drops the response message that a Gateway GPRS support node (GGSN) sends for a second Packet Data Protocol (PDP) context update.</p>
PAN-95148	<p>In an HA configuration, restarting the User-ID process (through the debug software restart process user-id CLI command) removes the IP address-port-user mappings of disconnected Terminal Services (TS) agents as expected on the primary firewall, but HA synchronization does not remove those mappings from the secondary firewall.</p> <p>Workaround: Restart the User-ID process on the secondary firewall.</p>
PAN-95028	<p>For administrator accounts that you create in PAN-OS 8.0.8 and earlier releases, the firewall does not apply password profile settings (Device > Password Profiles) until you upgrade to PAN-OS 8.0.9 or a later release and modify the account passwords. Administrator accounts that you create in PAN-OS 8.0.9 or a later release don't require you to change the passwords to apply password profile settings.</p>
PAN-94966	<p>After you delete disconnected and connected Terminal Server (TS) agents in the same operation, the firewall still displays the IP address-to-port-user mappings (showuser ip-port-user-mapping CLI command) for the disconnected TS agents you deleted (Device > User Identification > Terminal Services Agents).</p>

Issue ID	Description
	Workaround: Do not delete both disconnected and connected TS agents in the same operation.
PAN-94917 This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues .	On Panorama Log Collectors, the showsystem masterkey-properties CLI command does not display the master key lifetime and reminder settings.
PAN-94853 This issue is now resolved. See PAN-OS 8.0.10 Addressed Issues .	Mobile endpoints that use GPRS Tunneling Protocol (GTP) lose GTP-U traffic because the firewall drops all GTP-U packets as packets without sessions after receiving two GTP requests with the same tunnel endpoint identifiers (TEIDs) and IP addresses.
PAN-94846	When DPDK is enabled on the VM-Series firewall with i40e virtual function (VF) driver, the VF does not detect the link status of the physical link. The VF link status remains up, regardless of changes to the physical link state.
PAN-94777 This issue is now resolved. See PAN-OS 8.0.14 Addressed Issues .	A 500 Internal Server error occurs for traffic that matches a Security policy rule with a URL Filtering profile that specifies a Continue action (Objects > Security Profiles > URL Filtering) because the firewall does not treat the API keys as binary strings. Workaround: Reboot the firewall.
PAN-94654 This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues .	The published applications page for GlobalProtect Clientless VPN displays a blank application icon instead of the custom Application Icon that you specify (Network > GlobalProtect > Portals > Clientless VPN > Applications > <application> > <application>).
PAN-94452 This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues .	The firewall records GPRS Tunneling Protocol (GTP) packets multiple times in firewall-stage packet captures (pcaps).
PAN-94382 This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues .	On the Panorama management server, the Task Manager displays Completed status immediately after you initiate a push operation to firewalls (Commit all) even though the push operation is still in progress.

Issue ID	Description
PAN-94290	(HA active/active configurations only) Fragmented packets are dropped when traversing a firewall.
PAN-94278 This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues .	A Panorama Collector Group forwards Threat and WildFire Submission logs to the wrong external server after you configure match list profiles with the same name for both log types (Panorama > Collector Groups > <Collector_Group> > Collector Log Forwarding > {Threat WildFire} > <match_list_profile>). Workaround: Configure match list profiles with different names for Threat and WildFire Submission logs.
PAN-94187	The firewall does not apply tag-based matching rules for dynamic address groups unless you enclose the tag names with single quotes ('<tag_name>') in the matching rules (Objects > Address Groups > <address_group>).
PAN-94167 This issue is now resolved. See PAN-OS 8.0.10 Addressed Issues .	Firewalls randomly retain IP address-to-username mappings even after receiving information via User-ID Redistribution that the mapping was deleted or expired.
PAN-94023 This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues .	The request system external-listshow type ip name <EDL_name> CLI command does not display external dynamic list entries after you restart the management server (<i>mgmtsvr</i>) process.
PAN-93937 This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues .	The management server process (<i>mgmtsvr</i>) on the firewall restarts whenever you push configurations from the Panorama management server.
PAN-93889	The Panorama management server generates high-severity System logs with the message <code>Syslogconnection established to server</code> after you configure Traps log ingestion (Panorama > Log Ingestion Profile) for forwarding to a syslog server (Panorama > Server Profiles > Syslog) and commit configuration changes (Commit > Commit to Panorama). Workaround: Disable Traps log ingestion.
PAN-93854	The VM-Series firewall for NSX randomly disrupts traffic due to high CPU usage by the <i>pan_task</i> process.

Issue ID	Description
<p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.</p>	
<p>PAN-93755</p>	<p>SSL decrypted traffic fails after you Enforce Symmetric Return in Policy Based Forwarding (PBF) policy rules (Policies > Policy Based Forwarding).</p>
<p>PAN-93753</p> <p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.</p>	<p>High log rates cause disk space on PA-200 firewalls to reach maximum capacity.</p>
<p>PAN-93522</p> <p>This issue is now resolved. See PAN-OS 8.0.10 Addressed Issues.</p>	<p>On firewalls in an HA configuration, traffic is disrupted because the dataplane restarts unexpectedly when the firewall concurrently processes HA messages and packets for the same session. This issue applies to all firewall models except the PA-200 and VM-50 firewalls.</p>
<p>PAN-93430</p> <p>This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.</p>	<p>The firewall web interface doesn't display Host Information Profile (HIP) information in HIP Match logs for end users who have Microsoft-supported special characters in their domains or usernames.</p>
<p>PAN-93410</p>	<p>PA-5200 Series firewalls send logs to the passive or suspended Panorama virtual appliance in Legacy mode in an HA configuration.</p> <p>Workaround: On the active Panorama, run the request log-fwd-ctrl device <firewall_serial_number> action start CLI command, where <i><firewall_serial_number></i> is the serial number of the firewall from which you want to send logs to Panorama.</p>
<p>PAN-93968</p>	<p>The firewall and Panorama web interfaces display vulnerability threat IDs that are not available in PAN-OS 8.0 releases (Objects > Security Profiles > Vulnerability Protection > <profile> > Exceptions). To confirm whether a particular threat ID is available in your release, monitor the release notes for each new Applications and Threats content update or check the Palo Alto Networks Threat Vault to see the minimum PAN-OS release version for a threat signature.</p>
<p>PAN-93318</p> <p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.</p>	<p>Firewall CPU usage reaches 100 per cent due to SNMP polling for logical interfaces based on updates to the Link Layer Discovery Protocol (LLDP) MIB (LLDP-V2-MIB.my).</p>

Issue ID	Description
PAN-OS 8.0.11 Addressed Issues.	<p>Workaround: Restart the <i>snmpd</i> process by running the debug softwarerestart process snmp CLI command. Note that restarting <i>snmpd</i> reduces the CPU usage to allow other operations, but does not prevent the issue from recurring the next time SNMP polling occurs for the LLDP-V2-MIB.my MIB.</p>
<p>PAN-93233 This issue is now resolved. See PAN-OS 8.0.10 Addressed Issues.</p>	<p>PA-7000 Series firewalls cause slow traffic over IPSec VPN tunnels when the tunnel session and inner traffic session are on different dataplanes because the firewalls reorder TCP segments during IPSec encryption.</p> <p>Workaround: Keep the tunnel session and inner traffic session on the same dataplane. To determine which dataplane the tunnel session uses, first run the show vpn tunnel name <tunnel_name> CLI command to see the tunnel identifier, and then run the showvpn flow tunnel-id <tunnel_id> command to display the dataplane (owner cpuid). To force the inner traffic session onto the same dataplane, run the setsession distribution-policy fixed <dataplane> command.</p>
<p>PAN-93207 This issue is now resolved. See PAN-OS 8.0.15 Addressed Issues.</p>	<p>The firewall reports the incorrect hostname when responding to SNMP get requests.</p>
<p>PAN-93005 This issue is now resolved. See PAN-OS 8.0.14 Addressed Issues.</p>	<p>The firewall generates System logs with high severity for Dataplane under severe load conditions that do not affect traffic.</p>
<p>PAN-92604 This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.</p>	<p>A Panorama Collector Group does not forward logs to some external servers after you configure multiple server profiles (Panorama > Collector Groups > <Collector_Group> > Collector Log Forwarding).</p>
<p>PAN-92564 This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.</p>	<p>After you upgrade the firewall to a PAN-OS 8.0 release, a small percentage of writable third-party SFP transceivers (not purchased from Palo Alto Networks®) can stop working or experience other issues. For firewalls that use third-party SFPs, Palo Alto Networks recommends that you do not upgrade to PAN-OS 8.0 until a maintenance release that addresses this issue becomes available. Additionally, after a maintenance release with this fix becomes available and you begin the upgrade process, do not reboot the firewall after you download and</p>

Issue ID	Description
	<p>install the PAN-OS 8.0 base image: wait until after you download and install the maintenance release before rebooting.</p> <p>For additional details, upgrade considerations, and instructions for upgrading your firewalls, see the PAN-OS 8.0 upgrade information.</p>
<p>PAN-92487</p> <p>This issue is now resolved. See PAN-OS 8.0.10 Addressed Issues.</p>	<p>Enabling jumbo frames (Device > Setup > Session) reduces throughput because:</p> <ul style="list-style-type: none"> • The firewalls hardcode the maximum segment size (TCP MSS) within TCP SYN packets and in server-to-client traffic at 1,460 bytes when packets exceed that size. • PA-7000 Series and PA-5200 Series firewalls hardcode the maximum transmission unit (MTU) at 1,500 bytes for the encapsulation stage when tunneled clear-text traffic and the originating tunnel session reside on different dataplanes.
<p>PAN-92366</p> <p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.</p>	<p>PA-5200 Series firewalls in an active/passive HA configuration drop Bidirectional Forwarding Detection (BFD) sessions when the passive firewall is in an initialization state after you reboot it</p> <p>Workaround: On the passive firewall, set the Passive Link State to Shutdown (Device > High Availability > General > Active/Passive Settings).</p>
<p>PAN-92268</p> <p>This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.</p>	<p>Fixed an issue on PA-7000 Series and PA-5200 Series firewalls where one or more dataplanes did not pass traffic when you ran several operational commands (from any firewall user interface or from the Panorama management server) while committing changes to device or network settings or while installing a content update.</p>
<p>PAN-92163</p> <p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.</p>	<p>Firewalls in an active/passive HA configuration take longer than expected to fail over after you configure them to redistribute routes between an interior gateway protocol (IGP) and Border Gateway Protocol (BGP).</p>
<p>PAN-92105</p> <p>This issue is now resolved. See PAN-OS 8.0.8 Addressed Issues.</p>	<p>Panorama Log Collectors do not receive some firewall logs and take longer than expected to receive all logs when the Collector Group has spaces in its name.</p> <p>Workaround: Configure Collector Group names without spaces.</p>
<p>PAN-92017</p> <p>This issue is now resolved. See</p>	<p>Log Collectors that belong to a collector group with a space in its name fail to fully connect to one another, which affects log visibility and logging performance.</p>

Issue ID	Description
PAN-OS 8.0.10 Addressed Issues.	Workaround: Configure Collector Group names without spaces.
PAN-91689 This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.	The Panorama management server removes address objects and, in the Network tab settings and NAT policy rules, uses the associated IP address values without reference to the address objects before pushing configurations to firewalls.
PAN-91421	The firewall dataplane restarts and results in temporary traffic loss when any process stops responding while system resource usage is running high.
PAN-91370 This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.	The firewall drops IPv6 traffic while enforcing IPv6 bidirectional NAT policy rules because the firewall incorrectly translates the destination address for a host that resides on a directly attached network. Workaround: Above the bidirectional rule in your NAT policy, add an NPTv6 rule that specifies no translation and matches the IPv6 address configured on the interface that the firewall uses for traffic to the directly attached network.
PAN-91361 This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues.	Client connections initiated with HTTP/2 fail during SSL Inbound Inspection decryption because the firewall removes the Application-Layer Protocol Negotiation (ALPN) extension within the server hello packet instead of forwarding the extension to the client. Workaround: Disable HTTP/2 support in the servers.
PAN-91238 This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues.	An Aggregate Ethernet (AE) interface with Link Aggregation Control Protocol (LACP) enabled on the firewall goes down after a cisco-nexus primary virtual port channel (vPC) switch LACP peer reboots and comes back up. Workaround: Set a hold time on the AE interface by running the debugl2ctrlld lacp set hold-time CLI command. The hold time (default is 15 seconds) specifies the delay before the firewall processes LACP protocol data units (PDUs) after LACP-enabled interfaces come up.
PAN-91236	The Panorama management server does not display new logs collected on M-Series Log Collectors because the logging search engine fails to register during system startup when logging disk checks and RAID mounting takes longer than two hours to complete.
PAN-91088 This issue is now resolved. See	(PAN-OS 8.0.6 and later releases) On PA-7000 Series firewalls in an HA configuration, the HA3 link does not come up after you upgrade to PAN-OS 8.0.6 or a later release.

Issue ID	Description
PAN-OS 8.0.10 Addressed Issues.	Workaround: Unplug and replug the HSCI modules.
PAN-91059 This issue is now resolved. See PAN-OS 8.0.16 Addressed Issues.	(PAN-OS 8.0.4 and later releases) GTP log query filters don't work when you filter based on a value of unknown for the message type or GTP interface fields (Monitor > Logs > GTP).
PAN-90565 This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.	(PAN-OS 8.0.4 and later releases) The firewall does not accept wildcards ("*") as standalone characters to match all IMSI identifiers when you configure IMSI Filtering in a GTP Protection profile (Objects > Security Profiles > GTP Protection).
PAN-90448 This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues.	PA-7000 Series and PA-5200 Series firewalls don't properly Rematch all sessions on config policy change for offloaded sessions (Device > Setup > Session). Workaround: After committing your latest changes, clear sessions that are in a discard state by running the clear session all filter state discard CLI command.
PAN-90347 This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.	On a PA-5000 Series firewall configured to use an IPSec tunnel containing multiple proxy IDs (Network > IPSec Tunnels > <tunnel> > Proxy IDs), the firewall drops tunneled traffic after clear text sessions are established on a dataplane other than the first dataplane (DPO). Workaround: Use Palo Alto Networks firewalls on both ends of the IPSec tunnel, or use one proxy ID per tunnel, or use only DPO for establishing clear text sessions (run the set session processing-cpu dp0 CLI command).
PAN-90301 This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.	(PAN-OS 8.0.4 and later releases) The firewall generates false positives during GTP-in-GTP checks because it detects some DNS-in-GTP packets as GTP-in-GTP packets. Workaround: Disable GTP-in-GTP protection in the GTP Protection profile (Objects > Security Profiles > GTP Protection).
PAN-90096 This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.	(PAN-OS 8.0.4 and later releases) Threat logs record incorrect IMSI values for GTP packets when you enable Packet Capture in Vulnerability Protection profiles (Objects > Security Profiles > Vulnerability Protection > <vulnerability_protection_profile> > Rules).

Issue ID	Description
<p>PAN-90048</p> <p>This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues.</p>	<p>Automatic commits fail after you configure Security policy rules that reference region objects for the source or destination and then upgrade the PAN-OS software.</p> <p>Workaround: Run the debug device-server reset id-manager type vsys-region CLI command to remove stale region data and then run the commit force configuration mode command.</p>
<p>PAN-89988</p> <p>This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.</p>	<p>The firewall dataplane intermittently restarts, causing traffic loss, after you attach a NetFlow server profile to an interface for which the firewall assigns an invalid identifier.</p>
<p>PAN-89794</p> <p>This issue is now resolved. See PAN-OS 8.0.14 Addressed Issues.</p>	<p>(PA-3050, PA-3060, PA-5000 Series, PA-5200 Series, and PA-7000 Series firewalls only in an HA configuration) Multicast sessions intermittently stop forwarding traffic after HA failover on firewalls with hardware offloading enabled (default).</p> <p>Workaround: Disable hardware offloading by running the set session offloadno CLI command and clear any multicast sessions that are already offloaded after failover by running the clearsession CLI command.</p>
<p>PAN-89715</p> <p>This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.</p>	<p>On PA-5200 Series firewalls in an active/passive high availability (HA) configuration, failover takes a few seconds longer than expected when it is triggered after the passive firewall reboots.</p> <p>Workaround: Configure the Ethernet 1/1 to 1/4 interfaces and set the Passive Link State to Auto.</p>
<p>PAN-89443</p>	<p>On PA-5200 Series firewalls, frequent changes in the fan speeds intermittently cause disk errors in the log drives. (In PAN-OS 8.0.10, the fix for PAN-93715 mitigates this issue but does not completely resolve it.)</p>
<p>PAN-88487</p> <p>This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.</p>	<p>The firewall stops enforcing policy after an automatic or manual refresh of an External Dynamic List (EDL) that has an invalid IP address or that resides on an unreachable web server.</p> <p>Workaround: Do not refresh EDLs that have invalid IP addresses or that reside on unreachable web servers.</p>
<p>PAN-88440</p> <p>This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.</p>	<p>A firewall configured as a DNS proxy server (Network > DNS Proxy) displays the following error when performing a name server lookup for any domain on MAC endpoints: <code>Got recursion notavailable.</code></p>

Issue ID	Description
PAN-OS 8.0.13 Addressed Issues.	
PAN-88292 This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.	On Panorama management servers in an HA configuration, the Log Collector that runs locally on the passive peer does not forward logs to syslog servers.
PAN-87990 This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.	The WF-500 appliance becomes inaccessible over SSH and becomes stuck in a boot loop after you upgrade from a release lower than PAN-OS 8.0.1 and try to upgrade to PAN-OS 8.0.5 or a later release.
PAN-87122 This issue is now resolved. See PAN-OS 8.0.8 Addressed Issues.	Running the clear session allfilter source CLI command eleven or more times simultaneously causes Bidirectional Forwarding Detection (BFD) flapping. Workaround: Run the clear session all filter source commands one at a time instead of as a batch.
PAN-86936 This issue is now resolved. See PAN-OS 8.0.9 Addressed Issues.	On Panorama Log collectors, logs are temporarily unavailable because the <i>vldmgr</i> process restarts.
PAN-86903	In rare cases, PA-800 Series firewalls shut themselves down due to a false over-current measurement. Workaround: To reduce the likelihood that this issue will occur, upgrade to PAN-OS 8.0.7 or a later release.
PAN-86882 This issue is now resolved. See PAN-OS 8.0.8 Addressed Issues.	The firewall dataplane slows significantly and, in some cases, stops responding if you use nested wildcards ("*") with "." or "/" as delimiters in the URLs of a custom URL category (Objects > Custom Objects > URL Category) or in the Allow List of a URL Filtering profile (Objects > Security Profiles > URL Filtering > <URL-filtering-profile> > Overrides). Workaround: The best practice is to use a single wildcard to cover multiple tokens or the caret (^) character to target a single token. For details, see https://live.paloaltonetworks.com/t5/Management-Articles/Nested-Wildcard-in-URLs-May-Severely-Affect-Performance/ta-p/61323 .

Issue ID	Description
<p>PAN-86672</p> <p>This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues.</p>	<p>In rare cases, a commit causes the disk to become full due to an incorrect disk quota-size value, which causes the firewall to behave unpredictably (for example, the web interface and CLI become unresponsive).</p> <p>Workaround: Restart the management server (<i>mgmtsvr</i>) process by running the debug software restart process management-server CLI command.</p>
<p>PAN-86624</p>	<p>The Panorama management server doesn't display an Override button for Objects > External Dynamic Lists in child device groups that inherit the objects from parent device groups.</p>
<p>PAN-86583</p> <p>This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.</p>	<p>The DHCP process restarts while you commit a configuration change to DHCP settings and, as a result, DHCP clients cannot receive IP addresses from a firewall configured as a DHCP server (Network > DHCP).</p>
<p>PAN-86226</p> <p>This issue is now resolved. See PAN-OS 8.0.7 Addressed Issues.</p>	<p>On PA-5000 Series firewalls running PAN-OS 8.0.5 or a later 8.0 release, insufficient proxy memory causes decryption failures and prevents users from accessing the GlobalProtect portal or gateway.</p>
<p>PAN-86210</p>	<p>On M-500 appliances, running an ACC report for a large amount of data causes Panorama to restart because of heartbeat failure.</p>
<p>PAN-86028</p> <p>This issue is now resolved. See PAN-OS 8.0.11 Addressed Issues.</p>	<p>(HA active/active configurations only) Traffic in a GlobalProtect VPN tunnel in SSL mode fails after Layer 7 processing is completed if asymmetric routing is involved.</p>
<p>PAN-85938</p> <p>This issue is now resolved. See PAN-OS 8.0.7 Addressed Issues.</p>	<p>PAN-OS removes the IP address-to-username mappings of end users who log in to a GlobalProtect internal gateway within a second of logging out from it.</p>
<p>PAN-85691</p>	<p>Authentication policy rules based on multi-factor authentication (MFA) don't block connections to an MFA vendor when the MFA server profile specifies a Certificate Profile that has the wrong certificate authority (CA) certificate.</p>

Issue ID	Description
<p>PAN-85410</p> <p>This issue is now resolved. See PAN-OS 8.0.14 Addressed Issues.</p>	<p>A firewall configured for GlobalProtect Clientless VPN has two issues:</p> <ul style="list-style-type: none"> • The firewall dataplane restarts when client cookies contain a path that does not start with a forward slash (/). • The firewall does not properly reinitialize client cookies that have a missing path and domain and instead uses values from previously received cookies.
<p>PAN-85299</p> <p>This issue is now resolved. See PAN-OS 8.0.7 Addressed Issues.</p>	<p>On firewalls in an active/passive HA configuration with link or path monitoring enabled, a failover resulting from a link or path failure intermittently causes PAN-OS to delete host, connected, static, and dynamic routes (both OSPF and BGP) from the forwarding information base (FIB) on the firewall peer that becomes active. The link or path failure also intermittently causes PAN-OS to send unnecessary BGP withdrawal messages to BGP peers.</p>
<p>PAN-85228</p>	<p>Even though PAN-OS 8.0.5 is the minimum supported release for VMware NSX plugin 2.0.0, a Panorama management server running an earlier release does not block you from installing that plugin. After you install the NSX plugin 2.0.0, a Panorama management server running PAN-OS 8.0.4 or an earlier release does not display the status of its connection with the NSX Manager.</p>
<p>PAN-85209</p>	<p>End users cannot access websites for which the firewall applies Decryption policy and uses Online Certificate Status Protocol (OCSP) to verify the status of certificates. The issue occurs in cases where the certificate cache on the firewall is modified during the access attempts.</p>
<p>PAN-85103</p> <p>This issue is now resolved. See PAN-OS 8.0.8 Addressed Issues.</p>	<p>The Panorama management server stops communicating with firewalls when the incoming log rate from firewalls exceeds the capacity of the Panorama buffers.</p>
<p>PAN-84792</p>	<p>Firewalls report an interface speed of zero for some interfaces instead of the maximum possible speed when you run an SNMP query for the ifHighSpeed object (OID 1.3.6.1.2.1.31.1.1.1.15).</p>
<p>PAN-84670</p>	<p>(PAN-OS 8.0.4 and later releases) When you disable decryption for HTTPS traffic, end users who don't have valid authentication timestamps can access HTTPS services and applications regardless of Authentication policy.</p> <p>Workaround: Create a Security policy rule that blocks HTTPS traffic that is not decrypted.</p>

Issue ID	Description
PAN-84642	On the Panorama management server, the Authentication Profile drop-down in authentication enforcement objects doesn't display any authentication sequences that you configured (Objects > Authentication).
PAN-84445 <i>This issue is now resolved. See PAN-OS 8.0.8 Addressed Issues.</i>	The firewall intermittently misidentifies the App-ID for SSL applications. This issue occurs when a server hosts multiple applications on the same port, and the firewall identifies traffic for an application using this port on the server and then inaccurately records other applications on this server-port combination as the previously identified application.
PAN-84406 <i>This issue is now resolved. See PAN-OS 8.0.8 Addressed Issues.</i>	On a firewall configured to collect username-to-group mappings from multiple LDAP servers over SSL/TLS-secured connections (Device > Server Profiles > LDAP), the firewall reboots because the User-ID process (<i>userid</i>) restarts several times during initialization.
PAN-84199 <i>This issue is now resolved. See PAN-OS 8.0.13 Addressed Issues.</i>	After you disable the Skip Auth on IKE Rekey option in the GlobalProtect gateway, the firewall still applies the option: end users with endpoints that use Extended Authentication (X-Auth) don't have to re-authenticate when the key used to establish the IPSec tunnel expires (Network > GlobalProtect > Gateways > <gateway> > Agent > Tunnel Settings).
PAN-84045	On VM-Series firewalls in an HA configuration with Data Plane Development Kit (DPDK) enabled, HA path monitoring failures and (in active/passive deployments) HA failover occurred. Workaround: Disable DPDK by running the set system setting dpdk-pkt-io off CLI command.
PAN-83900 <i>This issue is now resolved. See PAN-OS 8.0.12 Addressed Issues.</i>	The Panorama management server does not run ACC reports or custom reports because the <i>reportd</i> process stops responding when an administrator tries to access a device group to which that administrator does not have access.
PAN-83610	PA-5200 Series firewalls that use the network processor and have session offload enabled intermittently reset the checksum of UDP packets. Workaround: In PAN-OS 8.0.6 and later releases, you can disable session offload for UDP traffic by running the set session udp-offload no CLI command.


Issue ID	Description
PAN-83598	VM-Series firewalls cannot monitor more than 500 virtual machine (VM) information sources (Device > VM Information Sources).
PAN-83451	When you push licenses to managed firewalls (Panorama > Device Deployment > Licenses), the Panorama management server displays an incorrect error message (<code>LicenseFeatureUnknown</code>) along with the list of licenses that were successfully installed. You can ignore this error message because the licenses install successfully.
PAN-83146	You cannot apply the Trusted Root CA designation to certificates for which the Algorithm is Elliptic Curve DSA and the Digest is sha256 (Device > Certificate Management > Certificates).
PAN-83047	The firewall displays the following commit warning when you configure a GlobalProtect gateway with a Tunnel Interface set to the default tunnel interface (Network > GlobalProtect > Gateways > <gateway> > General) even after you enable IPv6: <code>Warning: tunnel tunnel ipv6 is not enabled.IPv6 addresswill be ignored!</code>
PAN-82942 This issue is now resolved. See PAN-OS 8.0.10 Addressed Issues .	The firewall reboots because the User-ID process (<code>userid</code>) restarts several times when endpoints, while requesting services that cannot process HTTP 302 responses (such as Microsoft update services), authenticate to Captive Portal through NT LAN Manager (NTLM) and immediately disconnect. Workaround: Don't configure Captive Portal to use NTLM authentication.
PAN-82278	Filtering does not work for Threat logs when you filter for threat names that contain certain characters: single quotation ('), double quotation ("), back slash (\), forward slash (/), backspace (\b), form feed (\f), new line (\n), carriage return (\r), and tab (\t).
PAN-82251 This issue is now resolved. See PAN-OS 8.0.7 Addressed Issues .	The VM-Series firewall on AWS GovCloud does not support bootstrapping.
PAN-82125 This issue is now resolved. See PAN-OS 8.0.7 Addressed Issues .	The firewall management plane or control plane continuously reboots after an upgrade to PAN-OS 8.0, and displays the following error message: <code>rcu_sched detected stallson CPUs/tasks</code> .

Issue ID	Description
<p>PAN-82117</p> <p>This issue is now resolved. See PAN-OS 8.0.7 Addressed Issues.</p>	<p>PA-5000 Series firewalls in an active/active HA configuration intermittently drop packets when the session owner and session setup are on different HA peers.</p>
<p>PAN-82109</p> <p>This issue is now resolved. See PAN-OS 8.0.3 Addressed Issues.</p>	<p>On VM-Series firewalls, the session capacity drops to 1,248 after you activate a capacity license.</p>
<p>PAN-81521</p>	<p>Endpoints failed to authenticate to GlobalProtect through Kerberos when you specify an FQDN instead of an IP address in the Kerberos server profile (Device > Server Profiles > Kerberos).</p> <p>Workaround: Replace the FQDN with the IP address in the Kerberos server profile.</p>
<p>PAN-81125</p>	<p>(PAN-OS 8.0.3 and later releases) On a firewall configured to connect to Terminal Services (TS) agents, importing a configuration file that does not define TS agent connections causes the User-ID service to stop responding (Device > Setup > Operations > Import named configuration snapshot).</p> <p>Workaround: Add an empty TS agent node <code><ts-agent/></code> under <code><devices><entry><vsys><entry></code> in the configuration file before importing it.</p>
<p>PAN-81061</p> <p>This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues.</p>	<p>PA-3000 Series firewalls intermittently drop long-lived sessions that are active during a content update if you immediately follow the update with an Antivirus or WildFire update.</p>
<p>PAN-80564</p>	<p>The <code>mgmtsvr</code> process and other processes repeatedly restart due to abnormal system memory usage when a connection failure occurs between the firewall and a syslog server that use TCP over SSL/TLS to communicate.</p> <p>Workaround: In PAN-OS 8.0.4 and later 8.0 releases, you can stop the continuous restarts by running the debug syslog-ngrestart CLI command to restart the <code>syslog-ng</code> process. Alternatively, for all PAN-OS 8.0 releases, you can use UDP for communication between the firewall and syslog server.</p>

Issue ID	Description
<p>PAN-79423</p>	<p>Panorama cannot push address group objects from device groups to managed firewalls when zones specify the objects in the User Identification ACL include or exclude lists (Network > Zones) and the Share Unused Address and Service Objects with Devices option is disabled (Panorama > Setup > Management > Panorama Settings).</p> <p>Workaround: After an explicit deny-all-and-log rule, create a security policy rule that includes the Address or Address Group objects. The deny-all-and-log rule handles all sessions not handled by any previous rule. The security policy rule containing the address objects, while it would never be used, allows you to push the address objects to managed firewalls.</p>
<p>PAN-79365</p> <p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>Pushing Panorama template configurations to VM-Series firewalls for NSX removes those firewalls as managed devices on the Panorama management server.</p> <p>Workaround: Make minor configuration changes to Panorama and select Commit > Commit and Push. Panorama then displays the VM-Series firewalls for NSX as managed devices. You can then select Config > Revert Changes to revert the minor configuration changes to Panorama.</p>
<p>PAN-79291</p> <p>This issue is now resolved. See PAN-OS 8.0.14 Addressed Issues.</p>	<p>An intermittent issue occurs with ZIP hardware offloading (hardware-based decompression) where firewalls identify ZIP files as threats when they are sent over Simple Mail Transfer Protocol (SMTP).</p>
<p>PAN-78718</p> <p>This issue is now resolved. See PAN-OS 8.0.6 Addressed Issues.</p>	<p>A PA-7000 Series firewall running PAN-OS 7.1.12, PAN-OS 7.0.17, or a PAN-OS 6.1 release (or an earlier PAN-OS 7.1 or PAN-OS 7.0 release) stops saving and displaying new logs due to a memory leak after a Panorama management server running PAN-OS 8.0 pushes a predefined GTP report that specifies a field that is unrecognized by the firewall running the earlier PAN-OS release (Monitor > Reports > Mobile Network Reports).</p>
<p>PAN-78224</p> <p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>The firewall truncates passwords to 40 characters when end users try to authenticate through RADIUS in the Captive Portal web form.</p>
<p>PAN-78055</p>	<p>On PA-220, PA-500, and PA-800 Series firewalls, VPN tunnel traffic intermittently fails because the <i>keymgr</i> stops processing sysd messages.</p>

Issue ID	Description
	<p>Workaround: Run the debugsoftware restart process keymgr CLI command to restart the keymgr process.</p>
<p>PAN-78034 This issue is now resolved. See PAN-OS 8.0.6 Addressed Issues.</p>	<p>The Threat logs that Zone Protection profiles trigger for packet type events do not record IMSI and IMEI values.</p> <p>Workaround: Select Monitor > Threat, click the spyglass icon for the Threat log to display additional details, and then double-click the related logs to see the IMSI and IMEI of the subscriber that triggered the Threat log.</p>
<p>PAN-77702 This issue is now resolved. See PAN-OS 8.0.5 Addressed Issues.</p>	<p>Dynamic address updates take several minutes to complete on a Panorama management server in NSX deployments.</p>
<p>PAN-77671 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>The firewall identifies traffic to www.online-translator.com as the translator-5 application instead of as web-browsing.</p>
<p>PAN-77595 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>PA-7000 Series and PA-5200 Series firewalls forward a SIP INVITE based on route lookup instead of Policy-Based Forwarding (PBF) policy.</p>
<p>PAN-77339 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>The SafeNet Client 6.2.2 does not support the necessary MAC algorithm (HMAC-SHA1) to work with Palo Alto Networks firewalls that run in FIPS-CC mode.</p>
<p>PAN-77213 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>The Panorama management server does not forward logs to a syslog server over TCP.</p>
<p>PAN-77125</p>	<p>PA-7000 Series and PA-5200 Series firewalls configured in tap mode don't close offloaded sessions after processing the associated traffic; the sessions remain open until they time out.</p>

Issue ID	Description
	<p>Workaround: Configure the firewalls in virtual wire mode instead of tap mode, or disable session offloading by running the set session offload no CLI command.</p>
<p>PAN-77116 This issue is now resolved. See PAN-OS 8.0.8 Addressed Issues.</p>	<p>After bootup, the firewall displays error messages such as Error: sysd_construct_sync_importer(sysd_sync.c:328):sysd_sync_regist (111) Unknown error code, even though the bootup is successful.</p> <p>Workaround: Ignore the error messages; they do not affect the firewall operations.</p>
<p>PAN-77062 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>Administrators with a custom role cannot delete packet captures.</p>
<p>PAN-77033 This issue is now resolved. See PAN-OS 8.0.3 Addressed Issues.</p>	<p>Using the debug skip-condor-reports no CLI command to force a Panorama management server running PAN-OS 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 running PAN-OS 8.0 to manage a PA-7000 Series firewall running a PAN-OS 7.0 release.</p>
<p>PAN-76832 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>Modifying a BFD profile configuration (Network > Network Profiles > BFD Profile) or assigning a different BFD profile (Network > Virtual Routers > BGP) in a virtual router causes the associated routing protocol (BGP) to flap.</p>
<p>PAN-76779 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>On the PA-5020 firewall, the dataplane restarts continuously when a user accesses applications over a GlobalProtect Clientless VPN.</p>
<p>PAN-76509 This issue is now resolved. See PAN-OS 8.0.5 Addressed Issues.</p>	<p>On firewalls with multiple virtual systems, custom spyware signatures work only on vsys1 (Objects > Custom Objects > Spyware).</p>
<p>PAN-76270 This issue is now resolved. See PAN-</p>	<p>Operations that require heavy memory usage on Log Collectors (such as ingesting logs at a high rate) cause some other processes to restart.</p>

Issue ID	Description
<p>OS 8.0.4 Addressed Issues.</p>	<p>Workaround: To make more memory available for processes other than logging and reporting, run the debug logdb show-heap-size <4-32> CLI command and set the memory heap to a lower size than the default 8GB.</p>
<p>PAN-76162</p> <p>This issue is now resolved. See PAN-OS 8.0.3 Addressed Issues.</p>	<p>A Panorama management server running a PAN-OS 8.0 release or a PAN-OS 7.1.8 or later 7.1 release does not display logs from PA-7000 Series firewalls running a PAN-OS 7.0 or 7.1 release.</p> <p>Workaround: Run the debug skip-condor-reports no command and then the debug software restart process reportd command on a Panorama management server running a PAN-OS 8.0 release so that it can successfully query PA-7000 Series firewalls running a PAN-OS 7.1 release.</p> <p> Do not use the debug skip-condor-reportsno command to work around this issue if you use Panorama running a PAN-OS 8.0 release to manage a PA-7000 Series firewall running a PAN-OS 7.0 release (see PAN-77033).</p>
<p>PAN-76058</p> <p>This issue is now resolved (requires content release version 718 or a later version). See PAN-OS 8.0.4 Addressed Issues.</p>	<p>When migrating URL categories from BrightCloud to PAN-DB, the Panorama management server does not apply the migration to pre-rules and post-rules.</p>
<p>PAN-75960</p> <p>This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues.</p>	<p>You cannot store the master key on an HSM in PAN-OS 8.0. Doing so causes the firewall to enter maintenance mode after a reboot and to require a factory reset for recovery.</p>
<p>PAN-75908</p> <p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>Multicast packets with stale session IDs cause the firewall dataplane to restart.</p>
<p>PAN-75881</p> <p>This issue is now resolved. See PAN-</p>	<p>A regression introduced in PAN-OS 8.0.0 and 8.0.1 intermittently causes the firewall dataplane to restart when combined with content updates. For details, including the relevance of content release version 709, refer to the associated Customer Advisory.</p>

Issue ID	Description
OS 8.0.2 Addressed Issues.	
PAN-75457	<p>(PAN-OS 8.0.1 and later releases) In WildFire appliance clusters that have three or more nodes, the Panorama management server does not support changing node roles. In a three-node cluster for example, you cannot use Panorama to configure the worker node as a controller node by adding the HA 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 fails and the cluster becomes unresponsive.</p>
PAN-74886 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.	<p>The Panorama management server does not push a shared address object to firewalls when the object is part of a dynamic address group that uses a tag.</p>
PAN-74652 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.	<p>After a firewall successfully installs a content update received from the Panorama management server, Panorama displays a failure message for that update when the associated job ID on the firewall is higher than 65536.</p>
PAN-74632 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.	<p>The firewall does not clear IP address-to-username mappings or username-to-group mappings after reaching the limit for the number of user groups (100,000), which causes commit failures with the following errors:</p> <pre data-bbox="532 1312 1453 1375">user-id is not registerd</pre> <p>and</p> <pre data-bbox="532 1470 1453 1564">user-ID manager was reset. Commit is required to reinitialize User-ID.</pre>
PAN-74293 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.	<p>The firewall drops application sessions after only 30 seconds of idle traffic instead of after the session timeout associated with the application.</p>
PAN-74139	<p>On the PA-500 firewall, insufficient memory allocation causes SSL decryption errors that result in SSL session failures, and Traffic logs</p>

Issue ID	Description
<p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>display the Session End Reason as decrypt - error or decrypt - cert - validation.</p>
<p>PAN-73964</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>You cannot upgrade VM-Series firewalls on AWS to PAN-OS 8.0.0 if they are deployed in an HA configuration.</p>
<p>PAN-73933</p> <p>This issue is now resolved. See PAN-OS 8.0.5 Addressed Issues.</p>	<p>The log receiver (<i>logrcvr</i>) process restarts due to a memory leak after the firewall performs a log query for correlation objects or reports and the query includes the Threat Category field.</p>
<p>PAN-73879</p> <p>This issue is now resolved (requires content release version 658 or a later version).</p>	<p>You cannot clone the strict file blocking profile in PAN-OS 8.0, although cloning the basic file blocking profile (or any other Security Profile types) works as expected (Objects > Security Profiles > File Blocking).</p>
<p>PAN-73877</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>On a firewall with multiple virtual systems, you cannot use the web interface to generate a SAML metadata file for Captive Portal or GlobalProtect; after you click the Metadata link associated with an authentication profile, no virtual systems are available to select.</p> <p>Workaround: Access the firewall CLI, switch to the virtual system where you assigned the authentication profile (setsystem setting target-vsyst <virtual_system>), and generate the metadata file (show sp-metadata [captive-portal global-protect] vsyst <value> authprofile <value> ip-hostname <value>).</p>
<p>PAN-73859</p> <p>This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues.</p>	<p>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).</p>
<p>PAN-73849</p>	<p>After you perform a factory reset or private data reset on a fresh installation of the Panorama virtual appliance, the Panorama > Plugins page does not display the pre-loaded VMware NSX plugin and therefore you cannot use the web interface to install the plugin.</p>

Issue ID	Description
	<p>Workarounds:</p> <ul style="list-style-type: none"> • Use the request plugins install vmware_nsx-<version> CLI command to install the plugin. • Download the plugin from the Palo Alto Networks Support Portal and then upload the plugin to Panorama. The web interface then displays the plugin for you to install.
<p>PAN-73579</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>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.</p> <p>Workaround: Commit changes to the firewall daily to ensure you always have the latest version of the malicious IP address feeds.</p>
<p>PAN-73545</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>When adding interfaces to a VM-300, VM-500, or VM-700 firewall, you must commit twice for traffic to pass normally.</p>
<p>PAN-73530</p>	<p>The firewall does not generate a packet capture (pcap) when a Data Filtering profile blocks files (Objects > Security Profiles > Data Filtering).</p>
<p>PAN-73401</p>	<p>(PAN-OS 8.0.1 and later releases) When you import a two-node WildFire appliance cluster into the Panorama management server, the controller nodes report their state as out-of-sync if either of the following conditions exist:</p> <ul style="list-style-type: none"> • You did 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 an HA pair. Adding a worker node would make the cluster a three-node cluster.) • You did not configure a service advertisement (either by enabling or not enabling advertising DNS service on the controller nodes). <p>Workaround: There are three possible workarounds to sync the controller nodes:</p> <ul style="list-style-type: none"> • 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. • Configure a worker list on the cluster controller: <pre>admin@wf500(active-controller)# set</pre>

Issue ID	Description
	<pre>deviceconfig cluster mode controller worker-list <worker-ip-address></pre> <p>(<i><worker-ip-address></i> is the IP address of the worker node you are adding to the cluster.) This creates a three-node cluster. After you import the cluster into Panorama, Panorama reports that the controller nodes are in sync. When you want the cluster to have only two nodes, use a different workaround.</p> <ul style="list-style-type: none"> • 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 or is not enabled. <pre>admin@wf500(active-controller)# set deviceconfig cluster mode controller service-advertisement dns-service enabled yes</pre> <p>or</p> <pre>admin@wf500(active-controller)# set deviceconfig cluster mode controller service-advertisement dns-service enabled no</pre> <p>Both commands result in Panorama reporting that the controller nodes are in sync.</p>
<p>PAN-73316</p>	<p>When you configure GlobalProtect to authenticate end users through RADIUS, the firewall web interface uses the <code>user@domain</code> format (instead of <code>domain\user</code>) to display users after they first log in.</p> <p>Workaround: After a HIP report is generated, the username format is normalized and updated to the correct format.</p>
<p>PAN-73307</p>	<p>When you use the ACC tab to view Tunnel Activity and you Jump to Logs, the Tunnel Inspection logs display <code>tunnel</code> as the tunnel type.</p> <p>Workaround: Remove tunnel type from the query in tunnel logs.</p>
<p>PAN-73291</p> <p>This issue is now resolved. See PAN-</p>	<p>When 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.</p>

Issue ID	Description
OS 8.0.1 Addressed Issues.	However, authentication fails for client certificates signed by a CA certificate that is not listed first in the Certificate Profile.
PAN-73254 This issue is now resolved. See PAN-OS 8.0.3 Addressed Issues.	After you install the VMware NSX plugin on Panorama in an HA deployment, Panorama does not automatically synchronize configuration changes between the HA peers unless you first update settings related to the NSX plugin. Workaround: Configure the NSX settings and commit your changes to Panorama.
PAN-73207 This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.	On a firewall that integrates with Okta Adaptive as the multi-factor authentication (MFA) vendor, you cannot use push notification as an authentication factor.
PAN-73168 This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.	After you configure the firewall web interface and the GlobalProtect portal that hosts Clientless VPN applications to share the same FQDN, your browser displays a 400Bad Request error when you try to access the web interface. Workaround: The best practice is to configure separate FQDNs for the firewall 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 web interface.
PAN-73006 This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.	When logging rates are high, the Monitor > App Scope > Change Monitor and Network Monitor reports sometimes fail to display data when you filter by Source or Destination IP addresses. Additionally, the Monitor > 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.
PAN-72894 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.	Panorama does not display HA firewalls (Panorama > Managed Devices) after the <i>configd</i> process stops responding.
PAN-72861	When you configure a PA-5200 Series or PA-7000 Series firewall to perform tunnel-in-tunnel inspection, which includes GRE keep-alive packets (Policies > Tunnel Inspection > Inspection > Inspect Options), and you run the clear session all CLI command while traffic is traversing a tunnel, the firewall temporarily drops tunneled packets.

Issue ID	Description
<p>PAN-72843</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>A commit failure occurs when you try to commit a configuration that enables GlobalProtect Clientless VPN on multiple GlobalProtect portals using different DNS proxies.</p> <p>Workaround: Restart the firewall dataplane and repeat the commit.</p>
<p>PAN-72402</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>After you configure a BGP IPv6 aggregate address with an Advertise Filter that has both a prefix filter and a next-hop filter, the firewall advertises only the aggregate address and does not advertise the specific routes that the Advertise Filter covers (Network > Virtual Routers > <router> > BGP > Aggregate > <address> > Advertise Filters > <advertise_filter>).</p> <p>Workaround: 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>
<p>PAN-72342</p> <p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>End users who ignore the Duo V2 authentication prompt until it times out can still authenticate successfully to a GlobalProtect portal configured for two-factor authentication.</p>
<p>PAN-71833</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>For a TACACS+ authentication profile, the output of the test authentication authentication-profile CLI command intermittently displays authentication/authorizationfailedfor user 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>
<p>PAN-71829</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>The PA-5000 Series firewall dataplane restarts when you change a certificate linked to GlobalProtect or change the minimum or maximum version of the TLS profile linked to GlobalProtect.</p>
<p>PAN-71765</p>	<p>When you use the Panorama management server to deactivate a VM-Series firewall, the deactivation completes successfully but the web interface does not update to show that deactivation is complete.</p> <p>Workaround: View deactivation status from Panorama > Managed Devices.</p>

Issue ID	Description
<p>PAN-71556</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>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.</p> <p>Workaround: Monitor the number of table entries and run the clear mac all CLI command or reboot as needed to clear the table.</p>
<p>PAN-71334</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>The PA-5200 Series firewall delays the transmission of audio/video streams for up to 10 seconds for VoIP calls that use Session Initiation Protocol (SIP).</p>
<p>PAN-71329</p>	<p>Local users and user groups created in the Shared location (all virtual systems) are not available for user-to-application mapping for GlobalProtect Clientless VPN applications (Clientless VPN > Applications on the GlobalProtect Portal).</p> <p>Workaround: Create users and user groups under a specific virtual system on firewalls with multiple virtual systems. On firewalls with a single virtual system (such as the VM-Series firewalls), users and user groups are created in Shared and are not configurable for Clientless VPN applications.</p>
<p>PAN-71271</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>When you start the log purging process after an upgrade to PAN-OS 8.0 but before starting the log migration, the log migration fails and the firewall drops new logs.</p> <p>You cannot work around this issue when the log purging process starts before the log migration. To determine whether log purging has begun, run the less mp-log es_purge.log CLI command, enter a forward slash ("/"), enter deleting, and check the output. If the output indicates any matches, you cannot migrate; otherwise, you can start the migration.</p>
<p>PAN-71215</p>	<p>Using the Panorama management server to deactivate a VM-Series firewall fails and causes the firewall to become unreachable after you configure Panorama to Verify Update Server Identity (Panorama > Setup > Services > Verify Update Server Identity) and you disable this setting on the firewall (Device > Setup > Services).</p> <p>Workaround: Ensure that you configure both Panorama and the VM-Series firewall to Verify Update Server Identity before you deactivate the firewall.</p>
<p>PAN-70906</p>	<p>If the PAN-OS web interface and the GlobalProtect portal are enabled on the same IP address, then when a user logs out of the GlobalProtect</p>

Issue ID	Description
	<p>portal, the administrative user is also logged out from the PAN-OS web interface.</p> <p>Workaround: Use the IP address to access the PAN-OS web interface and an FQDN to access the GlobalProtect portal.</p>
<p>PAN-70353</p> <p>This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues.</p>	<p>GlobalProtect Clientless VPN does not work when its host is a GlobalProtect portal that you configured on an interface with DHCP Client enabled (Network > Interfaces > <interface> > IPv4).</p> <p>Workaround: Configure the interface to use Static IP addresses.</p>
<p>PAN-70323</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>Firewalls running in FIPS-CC mode display the following error when you try to import SHA-1 certificate authority (CA) certificates even when the private key is not included:</p> <pre data-bbox="537 785 1455 940"> Import of <cert name> failed. Unsupported digest or keys used in F IPS-CC mode. </pre>
<p>PAN-70181</p> <p>This issue is now resolved. See PAN-OS 8.0.6 Addressed Issues.</p>	<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 also fail.</p> <p>Workaround: Monitor memory usage and restart the <i>mgmtsvr</i> process when <i>mgmtsvr</i> virtual memory exceeds 6GB or <i>mgmtsvr</i> resident memory exceeds 4GB.</p>
<p>PAN-70119</p> <p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>The firewall maps users to the Kerberos Realm defined in authentication profiles (Device > Authentication Profiles) instead of extracting the realm from Kerberos tickets.</p>
<p>PAN-70046</p>	<p>A standard 404 browser error displays if you try to use GlobalProtect Clientless VPN without the correct content release version.</p> <p>Workaround: 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>
<p>PAN-70027 (PLUG-216)</p>	<p>The output of the show objectregistered-IP all command does not include the Source of IP tag (service profile name and ID).</p>

Issue ID	Description
<p>This issue is resolved with the VMware NSX 1.0.1 plugin.</p>	
<p>PAN-70023</p>	<p>Authentication using auto-filled credentials intermittently fails when you access an application using GlobalProtect Clientless VPN.</p> <p>Workaround: Manually enter the credentials.</p>
<p>PAN-69932</p> <p>This issue is now resolved. See PAN-OS 8.0.5 Addressed Issues.</p>	<p>The Panorama web interface and CLI respond slowly when numerous NSX plugins are in progress.</p>
<p>PAN-69874</p> <p>This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues.</p>	<p>When the PAN-OS XML API sends user mappings with no timeout value to a firewall that has the Enable User Identification Timeout option disabled, the firewall assigns the mappings a timeout of 60 minutes instead of never (Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Cache).</p>
<p>PAN-69505</p>	<p>When viewing an external dynamic list that requires client authentication and you Test Source URL, the firewall fails to indicate whether it can reach the external dynamic list server and returns a URL access error (Objects > External Dynamic Lists).</p>
<p>PAN-69367</p> <p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>The firewall incorrectly generates packet diagnostic logs and captures packets for sessions that are not part of a packet filter (Monitor > Packet Capture).</p>
<p>PAN-69340</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<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>Workaround: Reboot the VM-Series firewall to activate session capacity (Device > Setup > Operations).</p>
<p>PAN-68974</p> <p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>On PA-3000 Series firewalls, you cannot configure a QoS Profile to have a maximum egress bandwidth (Egress Max) higher than 1Gbps for an aggregate group interface (Network > Network Profiles > QoS Profile).</p>

Issue ID	Description
PAN-68767	Panorama does not change the connection Status of an NSX manager (Panorama > VMware NSX > Service Managers) from Unknown to Registered due to a non-existent null value entry in the NSX manager response.
PAN-67950	<p>The firewall drops Encapsulating Security Payload (ESP) packets because IPsec sessions remain stuck in opening status when Extended Authentication (X-Auth) is enabled (Network > GlobalProtect > Gateways > <gateway> > Agent > Tunnel Settings).</p> <p>Workaround: Disable X-Auth for the VPN tunnel.</p>
<p>PAN-67544</p> <p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	When a multicast forwarding information base (MFIB) times out, the packet processing process (<i>flow_ctrl</i>) stops responding, which intermittently causes the firewall dataplane to restart.
PAN-67422	<p>(PAN-OS 8.0.1 and later releases) 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> show wildfire-appliance last-device-registration all serial-number <value></pre> <p>The <value> 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> show wildfire-appliance last-device-registration all serial-number 002001000099</pre> <p>Workaround: Run the show wildfire global devices-reporting-data command to show only firewalls that are reporting</p>

Issue ID	Description
	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.
PAN-66997 This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues .	On PA-7000 Series, PA-5200 Series, and PA-5000 Series firewalls, users who access applications over SSL VPN or IPSec tunnels through GlobalProtect experienced one-directional traffic.
PAN-66122 This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues .	Firewalls do not support tunnel content inspection in a virtual-system-to-virtual-system topology.
PAN-66032	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).
PAN-64725 This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues .	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. Workaround: Use the debug management-serverreport-namelookup disable CLI command to disable DNS lookups for reporting purposes and then restart the log receiver by running debug software restart process log-receiver .
PAN-63905 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues .	Installing a content update or committing configuration changes on the firewall causes RTP sessions that were created from predict sessions to move from an active state to a discard state.
PAN-63274 This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues .	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.

Issue ID	Description
<p>PAN-62820</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<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>
<p>PAN-62453</p>	<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: https://www.vmware.com/support/pubs/nsx_pubs.html.</p> <p>Workaround: 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>
<p>PAN-61840</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues.</p>	<p>The show global-protect-portal statistics CLI command is not supported.</p>
<p>PAN-61834</p> <p>This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues.</p>	<p>The firewall captures packets of IP addresses that are not included in the packet filter (Monitor > Packet Capture).</p>
<p>PAN-58872</p>	<p>The automatic license deactivation workflow for firewalls with direct internet access does not work.</p> <p>Workaround: Use the request license deactivate key features <name> mode manual CLI command to Deactivate a Feature License or SubscriptionUsingtheCLI. To Deactivate a VM, choose Complete Manually (instead of Continue) and follow the steps to manually deactivate the VM.</p>
<p>PAN-56217</p>	<p>When you configure multiple DNS proxy objects that specify for the firewall to listen for DNS requests on the same interface (Network > DNS Proxy > Interfaces), the firewall applies settings only for the first DNS proxy object.</p> <p>Workaround: Modify each DNS proxy object to specify a unique interface:</p>

Issue ID	Description
	<ul style="list-style-type: none"> • 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. • To modify a DNS proxy object configured with multiple interfaces, delete the interface that is shared with other DNS proxy objects, click OK to save the modified object, and then Commit.
PAN-55825	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.
PAN-55437	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).
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>Workaround: 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-54531 This issue is now resolved. See PAN-OS 8.0.4 Addressed Issues .	The firewall stops writing new Traffic and Threat logs to storage because the Automated Correlation Engine uses disk space in a way that prevents the firewall from purging older logs.
PAN-54254	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> .
PAN-53825	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 Template and a Device Group commit when you modify the zone configuration to ensure that the zones are available on the firewall.
PAN-53663	When you open the SaaS Application Usage report (Monitor > PDF Reports > SaaS Application Usage) on multiple tabs in a browser, each for a different virtual system (vsys), and you then attempt to export

Issue ID	Description
	<p>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>Workaround: Export only one PDF at a time and wait for that export process to finish before you trigger the next export request.</p>
<p>PAN-53601</p>	<p>A Panorama management server running on an M-Series appliance cannot connect to a SafeNet Network or nCipher nShield Connect hardware security module (HSM).</p>
<p>PAN-51969</p>	<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>Workaround: To push the Dynamic Address Group updates to the VM-Series firewalls, you must manually synchronize the configuration with the NSX Manager (Panorama > VMware Service Manager and select NSX Config-Sync).</p>
<p>PAN-51952</p>	<p>When 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 policy intermittently redirects traffic 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>Workaround: Ensure that members assigned to a security group don't overlap with another security group and that each security group is assigned to a unique NSX Security policy rule.</p>
<p>PAN-51870</p>	<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 set deviceconfig system type dhcp-client command, you must include each of the following parameters: accept-dhcp-domain, accept-dhcp-hostname, send-client-id, and send-hostname.</p>
<p>PAN-51869</p>	<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>
<p>PAN-51673</p>	<p>BFD sessions are not established between two RIP peers when there are no RIP advertisements.</p> <p>Workaround: Enable RIP on another interface to provide RIP advertisements from a remote peer.</p>

Issue ID	Description
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 the Panorama management server. This issue occurs intermittently on the NSX Manager when you define security policy rules to redirect traffic to the new service profiles that are available for traffic introspection, and results in the following error:</p> <pre data-bbox="537 485 1455 667"> Firewall configuration is not in sync with NSX Manager. Conflict with Service Profile Oddhost on service (Palo Alto Networks NGFW) when binding to host <name>. </pre>
PAN-51122	<p>On the VM-Series firewall, when you manually reset a heartbeat failure alarm on the vCenter server to indicate that the firewall is healthy (change color to green), the vCenter server does not trigger a heartbeat failure alarm again.</p>
PAN-50651	<p>On PA-7000 Series firewalls, you must configure one data port as a log card interface because the traffic and logging capabilities of this model exceed the capabilities of the management (MGT) 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 intermittently cannot 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>Workaround: Enable the firewall as a DNS proxy but don't specify an Interface for the DNS proxy object to use (Network > DNS Proxy > Interface).</p>
<p>PAN-50641</p> <p>This issue is now resolved. See PAN-OS 8.0.6 Addressed Issues.</p>	<p>Enabling or disabling BFD for BGP or changing a BFD profile that a BGP peer uses causes BGP to flap.</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>

Issue ID	Description
PAN-47969	<p>If you log in to the Panorama management server as a Device Group and Template administrator and you rename a device group, the Panorama > Device Groups page no longer displays any device groups.</p> <p>Workaround: 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>Workaround: 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>Workaround: 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>Workaround: 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 ACC > Network Activity tab, when you add the label Unknown as a global filter, the firewall adds the filter as A1 and the query results display A1 instead of Unknown.</p>
PAN-44400	<p>On a VM-Series firewall on a Citrix SDX server deployed in an active/active HA configuration, the link on a 1Gbps SFP port does not come up after successive HA failovers.</p> <p>Workaround: Use a 10Gbps SFP port instead of the 1Gbps SFP port.</p>
PAN-44300	<p>You cannot view WildFire analysis reports on firewalls running a PAN-OS 6.1 release that connect to a WF-500 appliance in Common Criteria mode running a PAN-OS 7.0 or later release.</p>
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</p>

Issue ID	Description
	<p>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>Workaround: PAN-OS 7.0 introduced enhancements to SSL Decryption 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 Block sessions with unsupported versions to disallow unsupported protocol versions (Objects > Decryption Profile > SSL Decryption > SSL Forward Proxy and/or SSL Inbound Inspection).</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>Workaround: 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-40714	<p>When you access Device > Log Settings on a firewall running a PAN-OS 7.0 or later release and then use the CLI to downgrade the firewall to a PAN-OS 6.1 or earlier release and reboot, an error message displays the next time you access Log Settings. This occurs because PAN-OS 7.0 and later releases display Log Settings 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 Log Settings 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 (Objects > Security Profiles > URL Filtering > URL Filtering profile > Settings).</p>
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</p>

Issue ID	Description
	<p>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>Workaround: To generate an on-demand report, click Run Now when you configure the custom report.</p>
<p>PAN-39501</p>	<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>Workaround: Commit a second time, which clears the old pool allocation.</p>
<p>PAN-38584</p>	<p>When you push configurations from a Panorama management server running PAN-OS 6.1 or a later release to firewalls running PAN-OS 6.0.3 or an earlier 6.0 release, the commits fail on the firewalls due to an unexpected Rule Type error. This issue is caused by the Rule Type setting in Security policy rules that was not included in the upgrade transform, and therefore the firewalls did not recognize the new rule types.</p> <p>Workaround: Upgrade Panorama to PAN-OS 6.1 or a later release only if you also plan to upgrade all managed firewalls running PAN-OS 6.0.3 or an earlier 6.0 release to PAN-OS 6.0.4 or a later release before pushing a configuration to the firewalls.</p>
<p>PAN-38255</p>	<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 debug software restart process management-server CLI command.</p>
<p>PAN-37511</p>	<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>
<p>PAN-37177</p>	<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 Panorama > Managed Devices.</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</p>

Issue ID	Description
	<p>active Panorama peer synchronizes the configuration. During this time, the passive Panorama peer will log a critical message:</p> <pre data-bbox="537 331 1455 417">vm-cfg: failed to process registration from svm device. vm-state: active.</pre> <p>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>Workaround: To reestablish the connection to the managed devices, commit your changes to Panorama (click Commit and select Commit Type: Panorama). 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 Combined Rules Preview dialog (select Policies > Security > Post Rules and Preview Rules) does not display post rules and local rules for managed firewalls.</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>
PAN-36730	<p>(VM-Series for NSX firewalls only) When deleting VM-Series firewalls, all virtual machines (VMs) are deleted successfully but intermittently a few instances remain in the datastore.</p> <p>Workaround: Manually delete the VM-Series firewalls from the datastore.</p>
PAN-36728	<p>(VM-Series for NSX firewalls only) NSX Security policy does not redirect traffic from newly added guests or virtual machines to the VM-Series firewall even when the guests belong to a security group and are attached to the NSX Security policy.</p> <p>Workaround: Reapply the NSX Security policy on the NSX Manager.</p>
PAN-36727	<p>The VM-Series firewall fails to deploy and displays the following error message:</p> <pre data-bbox="537 1665 1455 1719">Invalid OVF Format in Agent Configuration.</pre> <p>Workaround: Use the following command to restart the ESX Agent Manager process on the vCenter Server:</p>

Issue ID	Description
	<pre data-bbox="548 233 1453 285">/etc/init.d/vmware-vmx tomcat-restart.</pre>
<p>PAN-36433</p>	<p>When HA failover occurs on the Panorama management server while the VMware NSX Manager is deploying the VM-Series firewall for NSX, the licensing process fails and displays the following error:</p> <pre data-bbox="548 474 1453 558">vm-cfg: failed to process registration from svm device. vm-state: active.</pre> <p>Workaround: Delete the unlicensed instance of the VM-Series firewall on each ESXi host and redeploy the Palo Alto Networks next-generation firewall service from the NSX Manager.</p>
<p>PAN-36409</p>	<p>When viewing the Session Browser (Monitor > Session Browser), using the global refresh option (top-right corner) to update the list of sessions causes the Filters field to display incorrectly and clears any previously selected filters.</p> <p>Workaround: 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 using the global (or browser) refresh option.</p>
<p>PAN-36394</p>	<p>(VM-Series for NSX firewalls only) 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.</p>
<p>PAN-36393</p>	<p>When deploying the VM-Series firewall, the Task Console displays Error while enabling agent. Cannot complete the operation. See the event log for details. This error displays even on a successful deployment. You can ignore the message if the VM-Series firewall is successfully deployed.</p>
<p>PAN-36333</p>	<p>When you add or edit a service object, the web interface displays the incorrect port range for both source and destination ports: 1 - 65535. The correct port range is 0 - 65535 and specifying port number 0 for either a source or destination port is successful.</p>
<p>PAN-36088</p>	<p>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.</p>
<p>PAN-36049</p>	<p>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</p>

Issue ID	Description
	Ethernet port and the untagged Ethernet port. This issue was seen on some Linux OS versions such as Ubuntu.
PAN-35903	<p>When you edit a traffic introspection rule on the NSX Manager (to steer traffic to the VM-Series firewall), an <code>invalid (tcp) port number</code> error or <code>invalid (udp) port number</code> error displays when you remove the destination port (TCP or UDP).</p> <p>Workaround: 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>Workaround: 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>Workaround: Disable promiscuous mode.</p>
PAN-34966	<p>On a VM-Series for NSX firewall, when adding or removing a security group (container) that is bound to a Security policy, the Panorama management server does not get a dynamic update of the added or removed security group.</p> <p>Workaround: To get the latest update, select Panorama > VMware Service Manager and Synchronize Dynamic Objects to initiate a manual synchronization.</p>
PAN-34855	<p>On a VM-Series for NSX 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 causes 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</p>

Issue ID	Description
	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.
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"> • nCipher 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. • SafeNet Network—When losing connectivity to either or both HSMs in an HA configuration, the display of information from the showha-status or show hsm info command is blocked for 20 seconds.
PAN-31593	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.
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> CLI command.</p> <p>Workaround: Reboot Panorama management server (Panorama > Setup > Operations) to enable summary logs.</p>
PAN-29411	<p>On the Panorama management server, after switching Context to a managed firewall, you cannot upgrade the PAN-OS software.</p> <p>Workaround: Use the Panorama > Device Deployment > Software page to deploy software updates to firewalls.</p>
PAN-29385	<p>On an M-100 appliance, you cannot configure the IP address of the management (MGT) interface while the appliance operates as the secondary passive peer in an HA pair.</p> <p>Workaround: To set the IP address for the MGT interface, 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 IP header of syslog messages sent from the firewall does not include the hostname. However, some syslog implementations require this field to be present.</p> <p>Workaround: Enable the firewall to include its IP address as the hostname in the syslog header by selecting Send Hostname in Syslog (Device > Setup).</p>
PAN-28794	When the (MGT) interface on a Panorama Log Collector has an IPv4 address and you want to configure only an IPv6 address, you can use the Panorama web interface to configure the new IPv6 address but not to remove the IPv4 address.

Issue ID	Description
	<p>Workaround: On Panorama, configure the MGT interface with the new IPv6 address, push the configuration to the Log Collector, and test connectivity using the IPv6 address to ensure that you won't lose access when you remove the IPv4 address. To remove the IPv4 address, run the deletedeviceconfig system ip-address CLI command on the Log Collector and commit the change.</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.</p> <p>Workaround: Use the debug dataplane resetssl-decrypt exclude-cache 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 an 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.</p> <p>Workaround: Log in to each peer in HA and Test SCP server connection 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 (Device > Scheduled Log Export) to an SCP server, you must log in to each managed device and Test SCP server connection 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>On the Panorama web interface (Panorama > Master Key and Diagnostics) and CLI, attempts to reset the master key fail. However, this does not cause a problem when pushing a configuration from Panorama to a firewall because the keys don't have to match.</p>
PAN-20162	<p>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.</p>

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
WF500-4893 This issue is now resolved. See PAN-OS 8.0.15 Addressed Issues .	(RADIUS server profile configurations only) You cannot send a commit from a Panorama appliance running a PAN-OS 8.1 release to a WF-500 appliance running a PAN-OS 8.0 release because the RADIUS authentication protocol is incorrectly changed to CHAP authentication.
WF500-4636 This issue is now resolved. See PAN-OS 8.0.15 Addressed Issues .	In rare cases when you upgrade a WF-500 appliance from a PAN-OS 7.1 release to a PAN-OS 8.0 release, the disk partition becomes full due to the amount of data on the drive. When you try deleting the backup database to free up space, the debugwildfire reset backup-database-for-old-samples CLI command fails and displays the following error: Server error : Clientwf_devsvr not ready.
WF500-4635	(PAN-OS 8.0 releases only) In rare cases where the disk partition becomes full, the WF-500 appliance does not come up after you upgrade from a PAN-OS 7.1 release to a PAN-OS 8.0 release because data migration stops progressing, several processes don't start, and automatic commits don't occur.
WF500-4632	(PAN-OS 8.0 releases only) A WF-500 appliance with millions of reports does not come up after you upgrade from a PAN-OS 7.1 release to a PAN-OS 8.0 release because the data migration runs slowly, several processes don't start, and automatic commits don't occur.
WF500-4218 This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues .	As part of and after upgrading a WildFire appliance to a PAN-OS® 8.0 release, rebooting a cluster node (requestcluster reboot-local-node) sometimes results in the nodez going offline or failing to reboot. Workaround: Use the debug cluster agent restart-agent CLI command to bring the node back on line and to restart the cluster agent as needed.
WF500-4200	The Create Date shown when using the show wildfireglobal sample-status sha256 equal <hash> and showwildfire global sample-analysis CLI commands is two hours behind the actual time for WF-500 appliance samples.

Issue ID	Description
<p>WF500-4186</p> <p>This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues.</p>	<p>In a three-node WildFire appliance cluster, if you decommission the backup controller node or the worker node (request cluster decommission start) 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 show cluster membership command on the primary controller node shows:</p> <pre style="background-color: #f0f0f0; padding: 10px;">Service Summary: Cluster:offline, HA:peer-offline</pre> <p>In this state, the cluster does not function and does not accept new samples for processing.</p> <p>Workaround: Reboot the primary controller (run the request cluster reboot-local-node CLI command on the primary controller). After the primary controller reboots, the cluster functions again and accepts new samples for processing.</p>
<p>WF500-4176</p> <p>This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues.</p>	<p>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 (show wildfire globalsample-status sha256 equal <value>) even though the node no longer belongs to the cluster.</p>
<p>WF500-4173</p> <p>This issue is now resolved. See PAN-OS 8.0.2 Addressed Issues.</p>	<p>Integrated reports are not available for firewalls connected to a WF-500 appliance running in FIPS mode.</p>
<p>WF500-4166</p>	<p>In a WildFire appliance cluster with three or more nodes and with two controller nodes, when 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 show clustertask local CLI command displays the following error:</p> <pre style="background-color: #f0f0f0; padding: 10px;">Server error: Cannot connect to 'cluster-mgr' daemon, please check it is running. Status Report: <node-ip-address>: reported leader <ip-address>, age 0.</pre>

Issue ID	Description
	<p data-bbox="560 222 1429 283"><i><node-ip-address></i>: quit cluster due to too many controllers.</p> <p data-bbox="544 325 1404 357">Workaround: Perform the following tasks to workaround this issue:</p> <ol data-bbox="544 378 1429 714" style="list-style-type: none"> <li data-bbox="544 378 1339 451">1. Reconfigure the node to run in worker mode using the set deviceconfig cluster mode worker command. <li data-bbox="544 462 1429 556">2. Run the commit force command. (A standard commit operation fails and returns a message that the cluster manager is non-responsive.) <li data-bbox="544 577 1429 714">3. After the commit force operation succeeds, reboot the node using the request cluster reboot-local-node command. Until you reboot the node, the node's application services do not respond.
WF500-4132	<p data-bbox="544 756 1380 934">If you remove a node from a two-node WildFire appliance cluster by deleting the high availability (HA) configuration (delete deviceconfig high-availability) and the cluster configuration (delete deviceconfig cluster), the single remaining cluster node cannot process samples.</p> <p data-bbox="544 955 1421 1018">Workaround: Use either of the following workarounds to enable the remaining cluster node to process samples:</p> <ul data-bbox="544 1039 1453 1333" style="list-style-type: none"> <li data-bbox="544 1039 1453 1176">• Make the cluster node a standalone WildFire appliance—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 data-bbox="544 1186 1453 1333">• Recreate the cluster—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: <pre data-bbox="560 1375 1429 1837"> admin@WF-500# set deviceconfig cluster cluster-name <name> interface <cluster-communication-interface> node controller admin@WF-500# set deviceconfig high-availability enabled yes interface hal port <port> peer-ip-address <node-port-ip-address> 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 </pre>

Issue ID	Description
	<code><node-backup-ha-interface-ip-address></code>
<p>WF500-4098</p> <p>This issue is now resolved. See PAN-OS 8.0.1 Addressed Issues</p>	<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 (Service Summary and <code>wildfire-apps - service</code>) are suspended.</p> <p>Workaround: 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"> 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). <p>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.</p> <ol style="list-style-type: none"> 2. Failover the active controller so that it becomes the passive (backup) controller by running the <code>request cluster reboot-local-node</code> operational command on the active controller. 3. Wait for the former active controller to come up completely. Its new cluster role is the passive controller (as shown in the prompt). 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. 5. Decommission the node by running the <code>request cluster decommission start</code> command.
<p>WF500-4044</p>	<p>The Panorama management server doesn't support removing a node from a cluster.</p> <p>Workaround: Remove a node from a cluster locally.</p>
<p>WF500-4001</p>	<p>On the Panorama management server, you can configure an authentication profile and Add groups or administrators to the Allow List in the profile (Panorama > Authentication Profile > <auth-profile> > Advanced). However, WildFire appliances and appliance clusters</p>

Issue ID	Description
	<p>support only the all value for the groups in the allow list for an authentication profile. The analogous WildFire appliance CLI command is set shared authentication-profile <name> allow-list [all], with all as the only allowed parameter.</p> <p>When you try to push a configuration that specifies a group or name other than all in the authentication profile from Panorama to a WildFire appliance or appliance cluster, the push operation fails. However, Panorama > Managed WildFire Appliances or Managed WildFire Clusters indicates the Last Commit State is commit succeeded despite the failure. The Config Status indicates cluster nodes are Out of Sync and when you click commit succeeded, the Last Push State Details displays an error message.</p> <p>For example, if you Add a group named abcd to an authentication profile named auth5 in Panorama and then attempt to push the configuration to a WildFire appliance cluster, Panorama returns the following error: authentication-profile auth5 allow-list 'abcd' is not an allowed keyword. This is because WildFire appliances and appliance clusters see the allow list argument as a keyword, not as a variable, and the only keyword allowed is all.</p>
WF500-3966	<p>The request cluster join ip <ip-address> CLI command is not functional; don't use it.</p>
WF500-3935	<p>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.</p>
WF500-3892	<p>The request cluster reboot-all-nodes CLI command is not functional; don't use it.</p> <p>Workaround: To reboot all nodes in a cluster, reboot each node individually using the request cluster reboot-local-node command from the node's local CLI.</p>
WF500-1584	<p>When using a web browser to view a WildFire Analysis Report from a firewall that uses a WF-500 appliance for file sample analysis, the report does not display 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.</p> <p>Workaround: Browse to the IP address or hostname of the WF-500 appliance, which will temporarily download the certificate into the</p>

Issue ID	Description
	browser. For example, if the IP address of the WF-500 is 10.3.4.99, open a browser and enter https://10.3.4.99 . You can then access the report from the firewall by selecting Monitor > Logs > WildFire Submissions , clicking log details , and then clicking WildFire Analysis Report .

PAN-OS 8.0 Addressed Issues

Review the issues that were addressed in each maintenance release of the PAN-OS 8.0 release.

For new features, associated software versions, known issues, and changes in default behavior in PAN-OS 8.0 releases, see the [PAN-OS 8.0 Release Information](#).

- > [PAN-OS 8.0.20 Addressed Issues](#)
- > [PAN-OS 8.0.19-h1 Addressed Issues](#)
- > [PAN-OS 8.0.19 Addressed Issues](#)
- > [PAN-OS 8.0.18 Addressed Issues](#)
- > [PAN-OS 8.0.17 Addressed Issues](#)
- > [PAN-OS 8.0.16 Addressed Issues](#)
- > [PAN-OS 8.0.15 Addressed Issues](#)
- > [PAN-OS 8.0.14 Addressed Issues](#)
- > [PAN-OS 8.0.13 Addressed Issues](#)
- > [PAN-OS 8.0.12 Addressed Issues](#)
- > [PAN-OS 8.0.11-h1 Addressed Issues](#)
- > [PAN-OS 8.0.11 Addressed Issues](#)
- > [PAN-OS 8.0.10 Addressed Issues](#)
- > [PAN-OS 8.0.9 Addressed Issues](#)
- > [PAN-OS 8.0.8 Addressed Issues](#)
- > [PAN-OS 8.0.7 Addressed Issues](#)
- > [PAN-OS 8.0.6-h3 Addressed Issues](#)
- > [PAN-OS 8.0.6 Addressed Issues](#)
- > [PAN-OS 8.0.5 Addressed Issues](#)
- > [PAN-OS 8.0.4-h2 Addressed Issues](#)
- > [PAN-OS 8.0.4 Addressed Issues](#)
- > [PAN-OS 8.0.3-h4 Addressed Issues](#)
- > [PAN-OS 8.0.3 Addressed Issues](#)
- > [PAN-OS 8.0.2 Addressed Issues](#)
- > [PAN-OS 8.0.1 Addressed Issues](#)
- > [PAN-OS 8.0.0 Addressed Issues](#)

PAN-OS 8.0.20 Addressed Issues

Issue ID	Description
PAN-115110	An enhancement was made to enable you to configure syslog parameters through the CLI debug command. To view the available parameters and change the configurations, run the debug syslogng-params settings CLI command and perform a commit force to apply the edits.
PAN-110304	Fixed an issue where the dataplane restarted due to a callback function, which caused a deadlock condition.
PAN-107779	Fixed an issue where Wildfire [®] signature version information was no longer displayed after you activated a GlobalProtect client.
PAN-106889	Fixed a rare issue on a firewall in a high availability (HA) active/passive configuration running in FIPS-CC mode where the passive firewall rebooted in to maintenance mode.
PAN-105437	Fixed an issue where a process (<i>userid</i>) ran out of file descriptors and stopped responding due to the rate of concurrent Security Assertion Markup Language (SAML) requests initiated by Authentication policy rules.
PAN-104163	Fixed an issue where the show config audit base-version CLI command continuously increased the number of file descriptors and caused a process (<i>mgmtsvr</i>) to exit and restart.
PAN-100773	(PA-7000 Series firewalls only) Fixed an issue where the Quad Small Form-factor Pluggable (QSFP) port on a 20GQ NPC card unexpectedly entered low power mode and did not link up.
PAN-99958	Fixed an issue where the dataplane did not receive enough keep-alive packets as expected, which caused the Syslog server connection to age-out.
PAN-99584	Fixed an issue where a PA-5200 Series firewall processed traffic that was in suspended mode.
PAN-94447	Fixed an issue where deleting all FQDN objects that are no longer in use did not remove them from the FQDN refresh table, which caused firewalls to continue resolving these old objects per the schedule.
PAN-50031	Fixed an issue where a process (<i>vm_decoynet</i>) stopped responding due to a race condition.

PAN-OS 8.0.19-h1 Addressed Issues

Issue ID	Description
PAN-123603	A security-related fix was made to prevent a memory corruption vulnerability in PAN-OS® software (PAN-SA-2019-0021 / CVE-2019-1580).
PAN-123564	A security-related fix was made to prevent a mitigation bypass that led to a remote code execution (RCE) vulnerability in PAN-OS® software (PAN-SA-2019-0022 / CVE-2019-1581).
PAN-123371	Fixed an issue where the Wildfire Analysis Report incorrectly displayed the following error message: You are not authorized to access this page on the web interface.

PAN-OS 8.0.19 Addressed Issues

Issue ID	Description
PAN-119745	A security-related fix was made to address the Netflix Linux kernel TCP SACK vulnerability (PAN-SA-2019-0013 / CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, and CVE-2019-5599).
PAN-118869	A security-related fix was made to address an issue where the php-debug log incorrectly displayed non-sanitized data (PAN-SA-2019-0019 / CVE-2019-1575).
PAN-107239	A security-related fix was made to address cleartext passwords and keys that were visible in the logs for XML API calls (PAN-SA-2019-0019 / CVE-2019-1575).

PAN-OS 8.0.18 Addressed Issues

Issue ID	Description
WF500-5023	Fixed an issue on WF-500 appliances where the cluster service took longer than expected to start due to a large number of queued sample data.
WF500-5022	Fixed an issue where a non-functioning CLI command was removed from WF-500 appliances.
WF500-4785	Fixed a rare issue on WF-500 appliances where the firewall did not respond after you upgraded the appliance from a PAN-OS 8.0.1 release to a PAN-OS 8.0.10 or later release. With this fix, you can run the new debug software raidfixup auto CLI command to recover the RAID controller.
PAN-116851	Fixed an issue where users were unable to open an app in their browser after they logged in to GlobalProtect™ Clientless VPN until they closed any and all tabs associated with that app and then opened the app a second time. This issue occurred only when an administrator configured a Source User for the Clientless VPN Security policy rule (Policies > Security > <GP-VPN-Security-policy-rule> > User).
PAN-113775	Fixed an issue where the firewall dropped UpdatePDPContext response packets and displayed the following GTP log event: 122113.
PAN-113631	A security-related fix was made to address a use-after-free (UAF) vulnerability in the Linux kernel (PAN-SA-2019-0017 / CVE-2019-8912).
PAN-113189	A security-related fix was made to correct log file string-conversion errors that caused parsing issues, which caused the User-ID (<i>userid</i>) process to stop running.
PAN-112319	Fixed an issue where a race condition caused a process (<i>mgmtsvr</i>) to restart with an error message: Connecting to management server failed.
PAN-111084	Fixed an issue where an out-of-memory condition caused all IPSec tunnels (which includes IKEv1, IKEv2, and NAT-T) to stop responding.
PAN-110390	Fixed an issue on PA-7000 Series firewalls where invalid filters caused the device management server to stop responding when you generated a database (DB) report from a remote firewall.

Issue ID	Description
PAN-110168	Fixed an issue where the firewall and Panorama™ web interface did not present HSTS headers to your web browser.
PAN-109663	Fixed an intermittent issue where the firewall dropped packets when the policy rule was set to allow but denied the packets during a commit or high availability (HA) sync.
PAN-109551	Fixed an issue where group-based policy match stopped responding after User-ID™ restarted.
PAN-109124	A security-related fix was made to address an issue where you were unable to retrieve GlobalProtect cloud service threat packet captures from the Logging Service on Panorama M-Series and virtual appliances.
PAN-108165	Fixed memory issues on Palo Alto Networks hardware and virtual appliances that caused intermittent management plane instability.
PAN-107708	Fixed an issue on a firewall where custom reports did not generate during intermittent times and were not sent to your email address.
PAN-106019	Fixed an issue where a process (<i>routed</i>) stopped responding when an incomplete command ran in the XML API.
PAN-104515	Fixed an issue where the Panorama web interface took longer than expected to update Managed Collectors (Panorama > Managed Collectors) status.
PAN-104264	Fixed an issue where the Panorama management server stopped responding when you upgraded from PAN-OS 8.0.9 to PAN-OS 8.1.3.
PAN-101955	Fixed an issue on an M-100 appliance in an HA configuration where administrators could not reestablish access to the appliance after a session ended unexpectedly.
PAN-101379	Fixed an issue where an invalid Captive Portal authentication policy was successfully pushed to managed firewalls, which caused autocommits to fail.
PAN-101289	Fixed an issue where simultaneous management access allowed only one user to log in at a time.
PAN-99016	A security-related fix was made to address the LazyFP state restore vulnerability (CVE-2018-3665 / PAN-SA-2019-0017).

Issue ID	Description
PAN-97496	Fixed an issue on a firewall where the (show runningresource-monitor ingress-backlogs) CLI command displayed invalid session IDs.
PAN-90738	Fixed an issue where a process (<i>configd</i>) exceeded the virtual memory usage limit and caused the firewall to restart. With this fix, you can run the following commands to avoid this unexpected restart: <ul style="list-style-type: none">• debug management-server system globalfinddisable-db-lookup – disables the default database lookup functionality.• debug management-server system appweb-thread-countenhance – increases appweb thread count to 200.
PAN-77977	Fixed an issue where a firewall configured with a regular expression data pattern (Objects > Custom Objects > Data Patterns > <profile-name> > Pattern Type) did not match patterns, which caused a memory leak and the firewall to stop responding.
PAN-63296	Fixed an issue where commits failed when a Panorama appliance running a PAN-OS 8.0 release pushed a template to a firewall running a PAN-OS 7.1 release due to file size limits.


PAN-OS 8.0.17 Addressed Issues

Issue ID	Description
WF500-4974	Fixed an issue on a WF-500 appliance where the static analysis results displayed in the PDF report but did not display in the WildFire® analysis summary of the web interface.
WF500-4784	Fixed an issue on a WF-500 appliance where during a reboot, the following error message displayed: FATAL: module nbd not found.
PAN-111048	Fixed an issue where the show object dynamic address group XML API command returned an invalid error message: You must specify a valid Device Group.
PAN-109668	A security related fix was made to limit the amount of information returned from an API call error message.
PAN-107659	(PA-5000 Series firewalls only) Fixed an issue where extra byte (1 to 7) padding were appended to the initial SYN and UDP packets, which caused the server to stop responding.
PAN-102954	A security-related fix was made to address a code parameter in the clientless VPN portal.
PAN-101391	Fixed an issue where the scheduled nightly custom report was not generated or emailed as expected.
PAN-99640	A security-related fix was made to address a denial of service (DoS) vulnerability in PAN-OS Linux Kernel (CVE-2017-8890).
PAN-99085	Fixed an issue where firewalls did not purge files automatically as expected, which caused WildFire updates to fail.

PAN-OS 8.0.16 Addressed Issues

Issue ID	Description
WF500-4397	Fixed an issue in a WF-500 appliance cluster where the controller backup node was stuck in <code>global-db-service: WaitingforLeaderReady</code> status when you tried to add nodes to the cluster.
WF500-4220	Fixed an issue on WF-500 appliances where the process (<code>rsyncd</code>) logs depleted root partition disk usage.
PAN-111866	Fixed an issue where the push scope selection on the Panorama web interface displayed incorrectly even though the commit scope displayed as expected. This issue occurred when one administrator made configuration changes to separate device groups or templates that affected multiple firewalls and a different administrator attempted to push those changes.
PAN-110341	Fixed an issue where the firewall sent RIP updates more frequently than expected.
PAN-110293	Fixed an issue where GTP-U traffic dropped when the GTP tunnel endpoint ID (TEID) was not updated correctly during a GTP-C update.
PAN-109594	Fixed an issue where the dataplane restarted when an IPsec rekey event occurred and caused a tunnel process (<code>tund</code>) failure when one--but not both--HA peers is running PAN-OS 8.0.14 or PAN-OS 8.1.5.
PAN-109506	Fixed an issue on a firewall where a process (<code>userid</code>) stopped responding due to excessive Security Assertion Markup Language (SAML) requests received.
PAN-107989	Fixed an issue on a firewall where the Strict IP Address Check incorrectly triggered when you enabled ECMP (Network > Virtual Routers > Add > Router settings > ECMP).
PAN-107895	Fixed an issue where PDP Delete Response packet did not match the GTPv1-C tunnel session, which caused the generated GTP log to display incorrect session data.
PAN-107636	(Panorama M-Series and virtual appliances only) Fixed a rare issue where the web interface did not display new logs as expected because Elasticsearch (ES) stopped working when the Raid drives reached maximum capacity and the purge script to remove old ES indices failed to execute and make room for new indices. However, this issue also resulted in creation of new ES indices that were empty because the

Issue ID	Description
	appliance could not read or write to them. With this fix, old indices are purged as expected; however, empty ES indices created before you upgraded to this release with this fix are not removed as expected (see known issue PAN-114041).
PAN-107144	Fixed an issue where you were unable to push to managed firewalls because the Push Scope field (Panorama > Managed Collectors > Commit > Push to Devices) did not display the managed firewalls.
PAN-107120	Fixed an issue on a firewall where the process (<i>all_pktproc</i>) failed, which caused the dataplane to restart.
PAN-106922	A security-related fix was made to address a denial of service (DoS) vulnerability in PAN-OS SNMP (CVE-2018-18065 / PAN-SA-2019-0007).
PAN-106857	Fixed an issue where the dataplane restarted due to an internal path monitoring failure due to large SSL decrypted file transfer sessions.
PAN-106253	Fixed an issue where the GTP Message Type Modify Bearer Response and GTP Event Code 124223 were denied due to failed stateful inspections.
PAN-106251	Fixed an issue where the list of Panorama Managed Devices did not display (Panorama > Device Deployment > Licenses).
PAN-105966	A security-related fix was made to address the Linux Kernel Local Privilege Escalation vulnerability (CVE-2018-14634 / PAN-SA-2019-0006).
PAN-105849	A security-related fix was made to address an issue with the <i>wf_curl.log</i> file in WF-500 appliances (WildFire).
PAN-105103	Fixed an intermittent issue where GTP logs did not display due to GTP packets with an APN > 14 bytes caused the traffic log to reach the limit and stopped generating logs.
PAN-104466	Fixed an issue on a VM-50 firewall where an out of memory event caused the firewall to restart.
PAN-104361	Fixed an issue on a firewall in an HA active/passive configuration where a process (<i>all_task</i>) failed due to a (<i>bad_gtp_header</i>) code on the passive firewall after upgrading from PAN-OS 8.0.12.
PAN-103225	Fixed an issue on Panorama M-Series and virtual appliances where after you push a configuration to a firewall, the Task Manager did not display the progress.

Issue ID	Description
PAN-103023	Fixed an intermittent issue where a content install (<i>content</i>) caused a firewall configuration failure and the firewall to stop responding.
PAN-102745	Fixed an issue on a firewall where a commit and FQDN refresh took longer than expected.
PAN-101451	Fixed an issue where SNMP queries displayed incorrect values.
PAN-101401	Fixed an issue where a DNS App-ID™ security policy allowed non-DNS traffic to flow through.
PAN-101365	Fixed an intermittent issue where the session ID did not clear when the session ID is set to 0.
PAN-100761	A security-related fix was made to address a development configuration file issue.
PAN-98861	Fixed an issue where shadowed rule warnings did not display during commits.
PAN-97879	Fixed an issue on Panorama management server in an HA active/passive configuration where a Commit (Commit > Commit to Panorama) caused the firewalls to restart.
PAN-97743	<p>Fixed an issue where the firewall did not recognize the small form-factor pluggable (SFP) port, which caused the dataplane to restart when the path monitor process stopped responding.</p> <p> <i>To ensure a successful upgrade to PAN-OS 8.0.16 for this fix, re-seat all connected SFP transceivers and then follow the upgrade path described in the PAN-OS 8.0 upgrade procedure (PAN-OS 8.0 New Features Guide).</i></p>
PAN-97634	Fixed an issue where the firewall rebooted when the management (MGT) interface was connected to a network that contained a network loop, which caused excessive traffic flow on the interface. This issue was observed only on a PA-220 firewall.
PAN-96344	Fixed an issue on a firewall where TCP reset packets were sent even after you set the vulnerability profile action to drop the packets.
PAN-96038	(PA-200, PA-220, and PA-220R firewalls only) Fixed an issue with the Ethernet driver that caused the firewall to reboot when experiencing heavy broadcast traffic on the management interface.

Issue ID	Description
PAN-91059	Fixed an issue where GTP log query filters did not work when you filtered based on a value of unknown for the message type or GTP interface fields (Monitor > Logs > GTP).
PAN-89849	Fixed an issue where the antivirus/anti-spyware block page did not display.
PAN-86319	Fixed an intermittent issue on M-100 appliances where the firewall became unresponsive when multiple users are logged in at the same time.
PAN-79090	Fixed an issue where HIP-related objects were missing transformation logic for OPSWAT on firewalls running a PAN-OS 8.0 release managed by a Panorama instance that was running a PAN-OS 8.1 release.
PAN-78262	Fixed an issue where the firewall did not display a shadow rule warning for security policy rules when a more broad rule is configured above a more specific rule.
PAN-73686	Fixed an issue where Security Assertion Markup Language (SAML) single sign-on (SSO) responses truncated group information when the field size exceeded 128 bytes, which caused the allow list check to fail.

PAN-OS 8.0.15 Addressed Issues

Issue ID	Description
WF500-4893	(RADIUS server profile configurations only) Fixed an issue where the RADIUS authentication protocol was incorrectly changed to CHAP authentication when you pushed a commit from a Panorama™ appliance running a PAN-OS® 8.1 release to a WF-500 appliance running a PAN-OS® 8.0 release.
WF500-4891	Fixed an issue on WF-500 appliances where the parsing script (sig_schedule_service) did not accurately identify specific WildFire® signatures.
WF500-4869	Fixed an issue on a WF-500 appliance where the sample analysis failed when using FIPS-CC mode.
WF500-4815	Fixed an intermittent issue on WF-500 appliances where the Redis command-line interface (CLI) failed to execute during master node re-balancing.
WF500-4664	Fixed an issue where the WF-500 appliance SNMP notifications did not provide information for the eth2 and eth3 interfaces.
WF500-4636	(WF-500 Appliances only) Fixed a rare issue that occurred after upgrading from a PAN-OS 7.1 release to a PAN-OS 8.0 release where the disk partition became full due to the amount of data on the drive and, when you tried to delete the backup database to free up space, the debug wildfire reset backup-database-for-old-samples CLI command failed and resulted in the following error: Server error : Client wf_devsrvr not ready.
PAN-108161	Fixed an issue on a high availability (HA) active/passive configuration where GTP sessions did not properly sync to the passive firewall, which caused a failure on the passive firewall during a failover.
PAN-107893	Fixed an issue where a Delete PDP Context Response (Monitor > Logs > GTP) did not correlate with a Delete PDP Context Request and appeared as a new session.
PAN-107790	Fixed an issue where Application incorrectly displayed as unknown-udp instead of gttp-c for theGTPv1-C tunnel management message GTP Event Type.
PAN-107734	Fixed an intermittent issue where IPSec Tunnels failed due to a race condition between the <i>pan_task</i> process and <i>tund</i> process.

Issue ID	Description
PAN-107290	Fixed an issue where a single API call failed to create a child device group under the parent device group.
PAN-107262	A security-related fix was made to prevent cross-site scripting (XSS) attacks through the PAN-OS Management Web Interface (CVE-2019-1566).
PAN-106776	A security-related fix was made to prevent a cross-site scripting (XSS) vulnerability in PAN-OS External Dynamic Lists (CVE-2019-1565).
PAN-105926	Fixed an intermittent issue on Panorama M-Series and virtual appliances where an address object referenced in the address group was allowed to be deleted without a reference error which caused commits to fail.
PAN-105695	Fixed an intermittent issue where the dataplane restarted while processing SMTP traffic.
PAN-105012	Fixed an issue on Panorama M-Series and virtual appliances where a log migration from an old-disk pair to a new-disk pair failed with the following error message: Error restoring disks from RMAed device, which caused the (<i>configd</i>) process to fail.
PAN-104668	Fixed an issue where a GTP PDP update did not update the GTP-U session which caused subsequent GTP traffic to drop.
PAN-103665	Fixed an issue on a high availability (HA) active/active configuration where the active primary LLDP profile could not be copied to the active secondary firewall.
PAN-101882	Fixed an issue on Panorama M-Series and virtual appliances where a partial Commit and Push for one or more administrators incorrectly sets the Push scope to all relevant firewalls as if a full Commit and Push was performed.
PAN-101607	Fixed an issue where template administrators with the required permission made configuration changes on shared objects and the Commit failed with the following error message: No pending change to commit.
PAN-101158	Fixed a username case sensitivity issue, which caused GlobalProtect™ Clientless VPN application lists to return empty.
PAN-101029	Fixed an issue where routing traffic dropped due to an increased activity in global counter (<i>flow_fpga_rcv_egr_L3_NH_NF</i>) when an interface is moved from one virtual router to another.

Issue ID	Description
PAN-100962	Fixed an issue on Panorama M-Series and virtual appliances where the disk quota configuration exceeded a combined total of 100 percent when a Push was performed from Panorama due to value discrepancies between Panorama and the firewall.
PAN-100717	Fixed an issue where the (<i>configd</i>) process depleted memory when you deleted multiple security rules with an XML API call.
PAN-99742	Fixed an issue on a PA-500 Series firewall where SSL Forward Proxy was denied due to insufficient shared memory.
PAN-99079	Fixed an issue on Panorama M-Series and virtual appliances where Logging Service was enabled, traffic log filters with a variable length subnet mask did not display any logs.
PAN-99002	Fixed a rare issue where XML files with random file sizes failed to upload through API calls.
PAN-98885	Fixed an issue where high elastic search memory load caused the firewall not to display logs and reboot
PAN-97898	Fixed a rare issue where the traffic log did not generate data due to a negative log counter reading.
PAN-97670	Fixed an issue on a VM-Series firewall in a high availability (HA) active/passive configuration where after a reboot, the passive firewall sent ARP packets during the initialization state, which caused a traffic conflict with the active firewall.
PAN-96978	Fixed an issue where the GlobalProtect Clientless VPN and GlobalProtect Data options did not display as expected on Panorama (Template > Device > Dynamic Updates).
PAN-95975	Fixed an issue on a firewall in a high availability (HA) active/passive configuration where the scheduled antivirus content update failed due to a process (<i>mgmtsvr</i>) failure.
PAN-95114	Fixed an issue where TACACS+ authorization responded with <code>Illegal packet version</code> because a firewall was incorrectly sending <code>minor version 1</code> , which impacts TACACS+ servers and causes a failed authorization.
PAN-93207	Fixed an issue where the firewall reported the incorrect hostname when responding to SNMP get requests.

Issue ID	Description
PAN-93112	Fixed an issue on a PA-5200 Series firewall where small form-factor pluggable (SFP) ports only linked in auto negotiation mode.
PAN-88018	Fixed an issue on Panorama M-Series and virtual appliances where the firewall was not able to override the local device configuration and failed to apply Dynamic Updates with an interval set to none.

PAN-OS 8.0.14 Addressed Issues

Issue ID	Description
WF500-4811	Fixed an issue where WF-500 appliances displayed the wrong WildFire® content version (show system info) after a WildFire content update.
WF500-4645	Fixed an issue where RAID rebuilding after disk replacement either failed or took longer than expected.
PAN-106936	Fixed an issue where PA-800 Series firewalls intermittently restarted due to a kernel error.
PAN-106016	Fixed an issue on PA-800 Series firewalls where a kernel memory spike caused the firewall to restart.
PAN-105921	Fixed an issue with Panorama™ where administrators were unable to use the web interface to acquire a commit or config lock for device groups.
PAN-105724	Fixed an issue where the firewall did not generate a new random value in the TLS Server Hello message, which broke TLSv1.3 connections when SSL Forward Proxy decryption was enabled.
PAN-104524	Fixed an issue where the firewall logged data in the packet-diag log for IP addresses that you did not specify in the packet-capture filters when you enabled the tunnel:flow log feature.
PAN-104406	Fixed an intermittent issue where the replace device CLI command caused the configuration lock to stop responding.
PAN-104073	Fixed an issue where the replace device old <serial-number> new <serial-number> command caused the configuration (<i>configd</i>) daemon to stop responding.
PAN-103383	Fixed an issue where a firewall blocked SMTP traffic when processing ZIP files due to too many packet-process loops.
PAN-102943	Fixed an Issue where a process (<i>mgmtsvr</i>) failed on EDL refresh when configured over a Secured Socket Layer (SSL) connection.
PAN-102743	(PA-5250, PA-5260, PA-5000 Series, and PA-7000 Series firewalls only) Fixed an intermittent issue where GlobalProtect™ SSL sessions that were enforcing client certificate authentication failed to resume and caused an authentication failure.

Issue ID	Description
PAN-102337	Fixed an issue on Panorama virtual appliances in a high availability (HA) configuration where the elastic search script failed to identify the master node due to case sensitivity in the serial number that caused log-replication failures when you enabled log redundancy.
PAN-101704	(PAN-OS 8.0.8 and later releases only) Fixed an issue where a configured Layer 3 interface erroneously opened ports 28869/tcp and 28870/tcp on the IP address assigned to that Layer 3 interface.
PAN-101585	(The following PA-7000 Series NPCs only: PA-7000-20G-NPC, PA-7000-20GQ-NPC, PA-7000-20GXM-NPC, and PA-7000-20GQXM-NPC) Fixed an issue where an egress buffer overflow that impacted internal packet path monitoring caused a high availability (HA) failover. Additionally, enhancements were made to flow control communication between the traffic manager and flow engine components to improve system stability during periods of heavy traffic.
PAN-101378	Fixed an issue with firewalls in an HA active/passive configuration where the firewall processed traffic in a suspended state.
PAN-101371	Fixed an issue where an M-500 appliance still pushed the previously configured values even after you cleared the values in the Management Interface Settings (Device > Setup > Interfaces > Management) and configured new ones.
PAN-100244	Fixed an issue where a failed commit or commit validation followed by a non-user-committed event (such as an FQDN refresh, an external dynamic list refresh, or an antivirus update) resulted in an unexpected change to the configuration that caused the firewall to drop traffic.
PAN-100228	Fixed an intermittent issue on a PA-7000 Series firewall where auto-commits prematurely executed before all Network Processing Cards (NPCs) were detected and ready.
PAN-100144	Fixed an issue on PA-7000 Series firewalls in a high availability (HA) active/active configuration where after a HA failover event the IP address rule list continuously duplicated entries and resulted in slow response times from the firewall and, eventually, caused the Network Processing Cards (NPCs) to restart.
PAN-99965	Fixed an issue where SNMP Object identifier queries for hrStorageAllocationUnits returned negative values.
PAN-99861	Fixed an issue where SaaS application usage reports were empty when you used special characters in naming zones.

Issue ID	Description
PAN-99860	Fixed an issue on a PA-7000 Series firewall where the Network Processing Card (NPC) rebooted due to a memory allocation issue.
PAN-99643	Fixed an issue where a change in user-mapping information prevented the host information profile (HIP) from updating.
PAN-99582	Fixed an issue where a firewall in an HA active/passive configuration did not send the Bidirectional Forwarding Detection (BFD) administrator down status after a manual failover.
PAN-99211	Fixed an issue in an HA active/passive configuration where the hardware offload feature attempted to reinstall IPSec sessions for individual packets, which caused additional dataplane CPU loads on both the active and passive firewalls.
PAN-99204	Fixed an issue on Panorama M-Series and virtual appliances where a qualifier configured for a custom application signature displayed the following error message: Unauthorized request.
PAN-99161	Fixed an issue where a Captive Portal configured with RADIUS authentication failed when a username contained the "at" (@) character.
PAN-99110	Fixed an issue where a library (<i>libpam_pan.so</i>) did not handle incorrect passwords as expected.
PAN-99095	Fixed an issue in Panorama where a commit failed message appeared in the Template Last Commit column in the device management summary after a Panorama reboot or upgrade.
PAN-98933	Fixed an issue on an M-100 appliance in an HA active/passive configuration where the schedules (Device > Dynamic Updates) were unresponsive after a failover or restart of the active firewall.
PAN-98683	Fixed an issue where Path Monitoring for IPv6 ping packets was dropping packets.
PAN-98504	A security-related fix was made to address three OpenSSL vulnerabilities: CVE-2018-0732, CVE-2018-0737, and CVE-2018-0739.
PAN-98475	Fixed an issue on a firewall configured with RADIUS where the default timeout setting failed after an administrator entered credentials through the web interface.
PAN-98332	Fixed an issue where the firewall incorrectly forwarded packets to upstream devices when it had no ARP entry for the destination IP

Issue ID	Description
	address, which resulted in traffic outages caused by source MAC addresses that did not get updated as expected.
PAN-98263	Fixed an issue on a PA-5000 Series firewall where SNMP values for received and transmitted bytes for Aggregate Ethernet (AE) subinterfaces returned incorrect values.
PAN-98195	Fixed an issue on a PA-220 firewall in an HA active/passive configuration and with jumbo frames enabled (Device > Setup > Session) where configuration and dynamic updates failed to synchronize.
PAN-98116	Fixed an issue where PA-3000 Series firewalls passed file descriptors in a dataplane process (<i>pan_comm</i>) during content (apps and threats) installation and FQDNRefresh job execution, which caused the hardware Layer 7 engine to identify applications incorrectly.
PAN-98110	(PAN-OS® 8.0.8 and later releases) Fixed an issue where administrator setting did not change when appropriate after you imported a configuration.
PAN-97928	Fixed an issue where you could not set the Captive Portal session timeout (Device > Setup > Session) to 60 seconds or longer without causing a browser redirect.
PAN-97698	Fixed an issue where the firewall took longer than expected to update a URL category.
PAN-97199	A security-related fix was made to the way the Linux kernel handles exceptions associated with MOV to SS and POP to SS instructions (CVE-2018-8897).
PAN-96696	A security-related fix was made to prevent modification of attributes in a SAML Response packet.
PAN-96522	Fixed an intermittent issue where the firewall did not rotate error logs correctly, which caused disk space issues.
PAN-96462	Fixed an intermittent issue where a null pointer exception caused the configuration (<i>configd</i>) process to stop responding.
PAN-96440	Fixed an issue where the static route was not reinstalled if you modified the path-monitoring hold time while the timer was active.
PAN-96283	Fixed an issue where administrators with predefined roles and permission to save configuration changes were not able to save their changes.

Issue ID	Description
PAN-96200	Fixed an issue where PA-220 firewalls that were bootstrapped with a configuration that enabled jumbo frames did not change the packet buffer size as expected, which resulted in a dataplane restart.
PAN-96109	Fixed an issue where a Panorama appliance returned the following error: <code>mgmtsrvr: User restart reason - Virtual memory limit exceeded (8204808 > 8192000)</code> .
PAN-95935	Fixed an intermittent issue on a PA-7000 Series firewall where the GlobalProtect LSVPN tunnel monitoring failed during re-key, which caused satellites to disconnect.
PAN-95819	Fixed an issue where a firewall did not apply the configured NAT policy during a predicted RTSP session.
PAN-95566	Fixed an intermittent issue where a process (<i>mdb</i>) stopped responding after a file cleanup failure.
PAN-95131	Fixed an issue where administrators with Device Group and Template access were not able to modify the QoS interface (Network > QoS).
PAN-94777	Fixed an issue where a 500 Internal Server error occurred for traffic that matched a Security policy rule with a URL Filtering profile that specified a <code>continue</code> action (Objects > Security Profiles > URL Filtering) because the firewall did not treat the API keys as binary strings.
PAN-94532	Fixed an issue where a memory leak caused an out-of-memory (OOM) error.
PAN-94413	Fixed an issue on Panorama M-Series and virtual appliances where the hash of the shared policy was incorrectly calculated, which caused an in-sync shared policy status to display as out - of - sync.
PAN-93457	Fixed an issue where continuous renewal for a session that went into DISCARD state when the firewall reached its resource limit prevented the creation of new sessions that matched that DISCARD session.
PAN-93456	Fixed an intermittent issue where VPN tunnels terminated due to IKE manager failures.
PAN-93005	Fixed an issue where the firewall generated System logs with high severity for Dataplane under severe load conditions that did not affect traffic. With this fix, the System logs have low severity for Dataplane under severe load conditions that do not affect traffic.

Issue ID	Description
PAN-92740	Fixed an issue in an NSX environment where the Panorama management server displayed an incorrect number of tags under Dynamic Address Groups when you configured a static tag in one or more address groups.
PAN-92548	Fixed an intermittent issue where a race condition caused the Logging Service or WF-500 appliances to disconnect from or become unresponsive to firewalls or the Panorama management server.
PAN-92380	Fixed an issue where, when you tried to export a custom report and your Chrome or Firefox browser was configured to block popup windows, the firewall instead downloaded a Tech Support File to your client system.
PAN-92256	Fixed an issue where the firewall didn't Block sessions with unsupported cipher suites based on Decryption policy rules for SSL Inbound Inspection when the rules referenced a Decryption Profile with a list of allowed ciphers that didn't match the ciphers that the destination server specified (Objects > Decryption > Decryption Profile). With this fix, the firewall checks the ciphers of both the source client and destination server against the cipher list in Decryption profiles when evaluating whether to allow sessions based on Decryption policy.
PAN-91259	Fixed an issue where the predict session for the RMI-IIOP application was not created correctly, which caused server-to-client initiated sessions to traverse slow-path inspection and, eventually, policy rules denied the traffic associated with these sessions.
PAN-90164	Fixed an issue on PA-3000 Series firewalls where commits took longer than expected or failed because the <i>pan_comm</i> process stopped responding.
PAN-89794	Fixed an issue on PA-3050, PA-3060, PA-5000 Series, PA-5200 Series, and PA-7000 Series firewalls in an HA configuration where multicast sessions intermittently stopped forwarding traffic after HA failover on firewalls with hardware offloading enabled (default).
PAN-87152	Fixed an issue where the show running ippool command stopped responding due to a conflict with packet processing and caused the Aggregate Ethernet (AE) interface to fail.
PAN-86769	Fixed an issue where a firewall did not forward logs when using the category eq command-and-control filter.
PAN-86426	A security-related fix was made to SAML authentication.

Issue ID	Description
PAN-85410	Fixed two issues on a firewall configured for GlobalProtect Clientless VPN: <ul style="list-style-type: none">• The firewall dataplane restarted when client cookies contained a path that did not start with a forward slash (/).• The firewall did not properly reinitialize client cookies that had a missing path and domain and instead used values from previously received cookies.
PAN-80078	Fixed an intermittent issue where operational commands executed by continuous API calls caused the firewall to stop responding with the following error message: <code>op command for client timed out as client is not available.</code>
PAN-79291	Fixed an intermittent issue with ZIP hardware offloading where firewalls identified ZIP files as threats when they were sent over Simple Mail Transfer Protocol (SMTP).
PAN-71911	Fixed an issue where the <code>pan_task</code> process resulted in a closed socket state caused by DPDK queries that were not flushed as expected.

PAN-OS 8.0.13 Addressed Issues

Issue ID	Description
WF500-4466	Fixed an issue on WF-500 passive cluster members where file forwarding was incorrectly disabled, which prevented the passive firewall from uploading samples.
PAN-104116	Fixed an issue during a PAN-OS® upgrade where a hardware packet buffer leak caused firewall performance to degrade.
PAN-103132	A security-related fix was made to address the FragmentSmack vulnerability (CVE-2018-5391 / PAN-SA-2018-0012).
PAN-102750	Fixed an issue on a PA-5000 Series firewall where the dataplane restarts when multicast traffic matched a stale session on the offload processor that was not cleared as expected.
PAN-102664	Fixed an issue where a process (<i>rasmgr</i>) restarted when a satellite tunnel tear down command and a get user config command occurred simultaneously.
PAN-102631	Fixed an issue where a process (<i>rasmgr</i>) restarted multiple times, which caused the firewall to reboot.
PAN-102168	Fixed an issue where a PA-5200 Series firewall processed the tunnel-monitoring with profile-failover as having the tunnel status up and peers as down during initial configuration.
PAN-102140	Fixed an issue where Extended Authentication (X-Auth) clients intermittently failed to establish an IPSec tunnel to GlobalProtect gateways.
PAN-101182	Fixed an issue where a system failure occurred due to packet size exceeding the hardware limit.
PAN-100985	Fixed an issue with PA-5000 Series, PA-5200 Series, and PA-7000 Series firewalls where the firewall fails to clear cache for refreshing the FQDN list, which periodically results in an out of memory condition that forces the firewall to reboot.
PAN-100794	Fixed an issue where SNMP fan trays did not initialize as expected and prevented the SNMP manager from receiving fan tray information.

Issue ID	Description
PAN-100715	Fixed an issue on VM-Series firewalls where the dataplane stops processing traffic when attempting to transmit packets larger than the firewall maximum transmission unit (MTU).
PAN-100345	(PA-200, PA-220, PA-220R, PA-500, and PA-800 Series firewall only) Fixed an issue where a large number of group mappings caused the firewall to display out-of-memory (OOM) errors and restart.
PAN-99964	Fixed an issue on an M-100 appliance where a bulk set of commands timed out causing configuration locks and, while running any subsequent show commands, responded with the following message: Server error: Timed out while getting configlock. Please try again.
PAN-99780	Fixed an issue where the second virtual system (vsys) dropped TCP traffic that was out-of-order when that second vsys controlled the proxy session in a multi-vsyes configuration.
PAN-99590	Fixed an issue where the firewall did not return Captive Portal response pages as expected due to depletion of file descriptors.
PAN-99392	Fixed an issue where RADIUS VSA administrators were able to login for one hour after their VSA administrator role was removed on the RADIUS server.
PAN-99316	Fixed an issue where the SAP Success Factor app failed to load because the Cipher-cloud was configuring cookies with the "at" (@) character in the cookie name but Palo Alto Networks firewalls used the @ character as a separator for storing cookies locally, which caused the firewall to misinterpret the cookies.
PAN-98976	Fixed an intermittent issue where Captive Portal MFA failed and discarded new MFA requests.
PAN-98635	Fixed an issue on the Panorama™ centralized management server where the logs related to the clear-log system were not forwarded to the Syslog server.
PAN-98217	Fixed an issue where user-account group members in subgroups (n+1) were unnecessarily queried when nested level was set to n.
PAN-98189	Fixed an issue where firewall overrides configuration to not validate first ASN, resulting in multi-lateral BGP connection flaps peering over an internet exchange.

Issue ID	Description
PAN-97881	Fixed an issue where an administrator with the CLI Device Read privilege was able to discard a session that was revoked.
PAN-97324	Fixed an issue where values were missing in the URL field in the Data Filtering logs.
PAN-97315	Fixed an issue on Panorama M-Series and virtual appliances where the configuration (<i>configd</i>) process stopped responding after you entered a filter string and tried to Add Match Criteria for any Dynamic address group type (Objects > Address Groups).
PAN-97296	Fixed an issue where the Panorama web interface Group Mapping Settings took longer to load than expected when there were multiple device groups and each group reported to a different master device.
PAN-97253	Fixed an issue where audio failed for long-lived session initiated protocol (SIP) sessions subjected to six content updates.
PAN-97077	Fixed an issue on Panorama M-Series and virtual appliances where the report-generation process stopped responding due to a corrupt log record in the JSON query.
PAN-97045	Fixed an issue on PA-850 firewalls where the session rematch option failed to execute when you added an IP address to the External Dynamic List (EDL) block list.
PAN-96918	Fixed an issue where an unreachable DNS server due to aggressive timers increased the time of PPPoE negotiation and, in some cases, caused negotiation to fail.
PAN-96860	Fixed an issue where the processing of ZIP files in the firewall dropped traffic unexpectedly and logged a threat entry for SMTP traffic.
PAN-96796	Fixed an intermittent issue where session BIND messages were dropped in a Dynamic IP configuration.
PAN-96734	Fixed an issue where a process (<i>configd</i>) stopped responding during a partial revert operation when reverting an interface configuration.
PAN-96678	Fixed an issue on PA-800 Series firewalls where the web interface did not display or allow you to configure the bandwidth setting any higher than 1Gbps.
PAN-96645	Fixed an issue where generation of extraneous data filtering logs for SMB protocol traffic occurred without data filtering or file blocking securities rules in place.

Issue ID	Description
PAN-96579	Fixed an issue where the Syslog server received an incorrect vsys/port log message when multiple vsys systems, with the same profile name and different port numbers, are connected to a single syslog server.
PAN-96477	Fixed an issue where PA-5000 Series firewalls did not send an IGMP query immediately after an HA failover.
PAN-96130	Fixed an issue on a PA-800 Series firewall where fragmented packets caused the firewall to restart.
PAN-95970	Fixed an issue on a PA-500 firewall where the dataplane tunnel content pointer entered a NULL state and caused dataplane processes (<i>pan_comm</i> and <i>tund</i>) to stop responding, which caused the dataplane to restart.
PAN-95736	Fixed an issue where the <i>mprelay</i> process stopped responding when you performed a commit while the firewall identified flows that needed a NetFlow update.
PAN-95486	Fixed an issue with VM-Series firewalls on Azure where dynamic updates failed for the GlobalProtect™ Data File when you scheduled the updates using the management interface.
PAN-95407	Fixed an issue where an API call resulted in an incorrect response.
PAN-95331	Fixed an issue where a temporary flap on configured Aggregate Ethernet (AE) interfaces cleared the dataplane debug logs.
PAN-95265	Fixed an issue on a PA-220 firewall where exporting the device state from the Panorama command-line interface (CLI) included the default bidirectional forwarding detection (BFD) configuration, which caused a commit to fail on the firewall when uploading the device state.
PAN-95045	Fixed an issue where syslog messages that terminated with 0 prevented the firewall from identifying matching patterns in the message.
PAN-94654	Fixed an issue where the published applications page for GlobalProtect Clientless VPN displayed a blank application icon instead of the custom Application Icon that you specified (Network > GlobalProtect > Portals > Clientless VPN > Applications > <application> > <application>).
PAN-94382	Fixed an issue on the Panorama management server where the Task Manager displayed Completed status immediately after you initiated a push operation to firewalls (Commit all) even though the push operation was still in progress.

Issue ID	Description
PAN-94317	<p>Fixed the following LDAP authentication issues:</p> <ul style="list-style-type: none"> • Authentication failed for users who belonged to user groups for which you specified LDAP short names instead of long names in the Allow List of an authentication profile (Device > Authentication Profile). • When performing LDAP lookups based on entries in the Allow List of LDAP authentication profiles, the firewall treated unknown group names as usernames. • Authentication failed for users who belonged to multiple groups that you entered in the Allow List of different LDAP authentication profiles.
PAN-94278	<p>Fixed an issue where a Panorama Collector Group forwarded Threat and WildFire® Submission logs to the wrong external server after you configured match list profiles with the same name for both log types (Panorama > Collector Groups > <Collector_Group> > Collector Log Forwarding > {Threat WildFire} > <match_list_profile>).</p>
PAN-94043	<p>Fixed an issue where, when an administrator made and committed partial changes, the disabled address objects used in a disabled security policy were pushed from Panorama and retained on the firewall but were deleted when an administrator performed a full commit from Panorama.</p>
PAN-93469	<p>Fixed an issue where the GlobalProtect login, welcome, and help pages did not display custom logo images in any browsers other than Internet Explorer after you upgraded to PAN-OS 8.0.8 or a later release.</p>
PAN-93430	<p>Fixed an issue where the firewall web interface did not display Host Information Profile (HIP) information in HIP Match logs for end users who had Microsoft-supported special characters in their domains or usernames.</p>
PAN-93152	<p>Fixed an intermittent Panorama issue where, after upgrading to PAN-OS 8.0 or a later release and when connected to a WF-500 appliance, commit validations failed due to a mismatched threat ID range on the WildFire private cloud.</p>
PAN-92955	<p>Fixed an issue on PA-5200 Series firewalls in an HA active/active configuration where session timeouts occurred when TCP timers did not update as expected for asymmetric flows.</p>
PAN-92782	<p>Fixed an issue where administrators with virtual system-specific role privileges could use the PAN-OS XML API to commit changes to shared</p>

Issue ID	Description
	objects on the firewall. With this fix, only administrators with the superuser role can commit changes to shared objects.
PAN-92596	Fixed an issue where the output of the show neighborndp-monitorall CLI command was missing a space between the Interface and IPv6 Address columns, which decreased readability.
PAN-92553	Fixed an issue on the Panorama management server where filtering logs based on IPv6 sources didn't return the expected results (Monitor > Logs > <log_type>).
PAN-92489	Fixed an issue where firewalls intermittently forwarded logs directly to the Panorama management server instead of to Log Collectors after you pushed a Collector Group preference list to the Log Collectors.
PAN-90998	Fixed an issue on firewalls with SSL Inbound Inspection decryption enabled where the dataplane restarted because the firewall did not correctly handle TCP RST messages.
PAN-90347	Fixed an issue on a PA-5000 Series firewall configured to use an IPsec tunnel containing multiple proxy IDs (Network > IPsec Tunnels > <tunnel> > Proxy IDs) where the firewall dropped tunneled traffic after clear text sessions were established on a different dataplane than the first dataplane (DPO).
PAN-89988	Fixed an issue where the firewall dataplane intermittently restarted, causing traffic loss, after you attached a NetFlow server profile to an interface for which the firewall assigned an invalid identifier.
PAN-89715	Fixed an issue on PA-5200 Series firewalls in an HA active/passive configuration where failover took a few seconds longer than expected when it was triggered after the passive firewall rebooted.
PAN-89346	Fixed an issue where an XML API call to execute the show system raid detail CLI command returned an error.
PAN-88440	Fixed an issue where a firewall configured as a DNS proxy server (Network > DNS Proxy) displayed the following error when performing a name server lookup for any domain on MAC endpoints: Got recursion not available.
PAN-88292	Fixed an issue on Panorama management servers in an HA configuration where the Log Collector that ran locally on the passive firewall did not forward logs to syslog servers.

Issue ID	Description
PAN-87969	Fixed an issue where the firewall inserted hard-coded double quotes (") for the \$opaque macro in payloads after you configured log forwarding to a JSON-type HTTP server.
PAN-87867	Fixed an issue on an M-100 appliance where, when the interface and snapshot length (snaplen) options were enabled, the tcpdump command failed to execute with the following message: <code>Unsupported number of arguments.</code>
PAN-87546	Fixed an intermittent issue where the User-ID™ (<i>userid</i>) process stopped responding and caused the firewall to restart.
PAN-87132	Fixed an issue on an M-100 appliance where a restart of the correlation (<i>cord</i>) process caused the appliance to reboot.
PAN-86759	Fixed an issue where the URL session information WildFire report displayed Unknown for sample files uploaded from firewalls running a PAN-OS 8.0 release.
PAN-86583	Fixed an issue where the DHCP process restarted while you committed a configuration change to DHCP settings and, as a result, DHCP clients could not receive IP addresses from a firewall configured as a DHCP server (Network > DHCP).
PAN-84199	Fixed an issue where, after you disabled the Skip Auth on IKE Rekey option in the GlobalProtect gateway, the firewall still applied the option: end users with endpoints that used Extended Authentication (X-Auth) did not have to re-authenticate when the key for establishing the IPsec tunnel expired (Network > GlobalProtect > Gateways > <gateway> > Agent > Tunnel Settings).
PAN-81553	Fixed an issue where the M-100 appliance used the default value of 1,000 because the maximum number of user groups was not defined in the system configuration.
PAN-81074	Fixed an issue on PA-7000 Series firewalls where the output from the REST/API version of the <code><show><system><raid><detail></code> command did not include all of the same output as the CLI version of this command.
PAN-80505	Fixed an issue where a firewall was able connect to Panorama using an expired certificate.

PAN-OS 8.0.12 Addressed Issues

Issue ID	Description
PAN-100870	Fixed an issue where the GlobalProtect™ app incorrectly displays a warning (Password Warning: Password expires in 0 days) even though the password has not, yet, expired.
PAN-99968	Fixed an issue where the firewall incorrectly dropped GTPv2-C Modify Bearer Response packets due to a sequence-number mismatch.
PAN-99897	Fixed an issue where a configuration change commit was accepted when only one virtual wire (vwire) interface was defined in a vwire pair. With this fix, a commit for a change where only one vwire interface is defined for a vwire pair is rejected and an error message is displayed.
PAN-99380	Fixed an issue where the dataplane stopped responding when a tunnel interface on the firewall received fragmented packets.
PAN-99263	Fixed an issue where NetFlow caused an invalid memory-access issue that caused the <code>pan_task</code> process to stop responding.
PAN-99212	Fixed an issue where the firewall incorrectly dropped ARP packets and increased the <code>flow_arp_throttle</code> counter.
PAN-99141	Fixed an issue in an HA active/active virtual wire configuration where a race condition caused the firewall to intermittently drop First SYN packets when they traversed the HA3 link.
PAN-99067	Fixed an issue where a firewall frequently flapped a BGP session when the firewall did not receive any response from the BFD peer or when BFD was configured only on the firewall.
PAN-99060	Fixed an issue where searching through pcaps from a Log Collector in a configuration with multiple Log Collectors took longer than expected.
PAN-98949	Fixed an issue on Panorama™ where generating a threat pcap from the web interface (Monitor tab) took longer than expected and caused the web interface and CLI to become inaccessible.
PAN-98479	Fixed an issue where Panorama displayed a <code>File not found</code> error when you attempted to view or download Threat packet captures (pcaps) from the Monitor tab.

Issue ID	Description
PAN-98470	Fixed an issue on a firewall with GTP stateful inspection enabled where the firewall incorrectly identified GTP echo packets as GTP-U application packets.
PAN-98097	Fixed an issue on PA-3000 Series, PA-3200 Series, PA-5000 Series, PA-5200 Series, and PA-7000 Series firewalls where Captive Portal was inaccessible for traffic on Secure HTTP (https) websites when SSL decryption was enabled and users were behind a proxy server.
PAN-97905	Fixed an issue where device-group operations were discarded when a concurrent commit was triggered by a different administrator.
PAN-97208	Fixed an issue where a firewall in a high availability (HA) active/active virtual wire (vwire) configuration with SSL decryption enabled passed traffic through the wrong firewall.
PAN-96997	Fixed an intermittent issue where detecting an unreachable WF-500 node took longer than expected.
PAN-96889	Fixed an issue where administrators were required to perform a commit force before pushing a partial or regular commit operation to managed appliances when the management server (<i>mgmtsvr</i>) or configuration (<i>configd</i>) process encountered a virtual memory leak and restarted.
PAN-96737	Fixed an issue with an incorrect policy match because Google-docs-base was incorrectly identified as SSL.
PAN-96572	Fixed an issue where, after end users successfully authenticated for access to a service or application, their web browsers briefly displayed a page indicating authentication completed and then they were redirected to an unknown URL that the user did not specify.
PAN-96565	Fixed an issue where the DNS proxy process failed due to a DNS response packet containing a TXT resource record with length = 0.
PAN-96431	A security-related fix was made to prevent HTTP Header Injection in the Captive Portal.
PAN-96388	Fixed an issue in a non-vsyst configuration where a firewall dropped the Client Hello packet from tunneled traffic when inbound decryption was enabled because the firewall considered that packet to be an inter-vsyst inbound packet.
PAN-96231	Fixed an issue where a commit took significantly longer than expected when cloning a rule compared to when configuring a new rule when the configuration contained a large number of rules.

Issue ID	Description
PAN-96113	Fixed an issue where the show routing protocol bgp rib-out CLI command did not display advertised routes that the firewall sent to the BGP peer. This issue was observed only in a deployment where a firewall is connected to a Border Gateway Protocol (BGP) peer that advertised a route for which the next hop is not in the same subnetwork as the BGP peer interface.
PAN-95999	Fixed an issue where firewalls in an HA active/active configuration with a default session setup and owner configuration dropped packets in a GlobalProtect VPN tunnel that used a floating IP address.
PAN-95766	Fixed an issue where Q-in-Q-tagged packets passed through a firewall without inspection or session creation.
PAN-95730	Fixed an issue where a firewall dropped SIP-RTP packets flowing through a GRE tunnel when a Tunnel Inspection Policy was configured with Security Options (Tunnel Inspection zones).
PAN-95712	Fixed an issue where browsers failed to load custom response pages on decrypted websites when those pages were larger than 8,191 bytes. With this fix, the firewall supports decryption of custom response pages up to 17,999 bytes.
PAN-95698	Fixed an issue where the firewall revealed part of a password in cleartext on the command-line interface (CLI) and management server (<i>mgmtsvr</i>) log when an administrator attempted to set a password that exceeded the maximum number of characters (31) using the CLI. With this fix, the firewall reports an error when an administrator attempts to set a password that contains more than 31 characters without revealing any part of the actual password.
PAN-95439	Fixed an issue where using the test nat-policy-match command from the XML API does not result in any matches when the matching policy is a destination NAT policy.
PAN-95339	Fixed an issue where a firewall sent packets out of order when the sending rate was too high.
PAN-95090	Fixed an issue where imported custom applications did not display in Security Policies that were created through the web interface.
PAN-95061	Fixed an issue on PA-220 firewalls where either a commit or an EDLRefresh job failed with the following error message: <code>failed to handle CONFIG_UPDATE_START</code> . This issue occurred after an increase in the number of type URL entries in an external dynamic list.

Issue ID	Description
PAN-94917	Fixed an issue on Panorama Log Collectors where the show system masterkey-properties CLI command did not display the master key lifetime and reminder settings.
PAN-94582	Fixed an issue where the firewall did not correctly re-learn a User-ID™ mapping after that mapping was temporarily lost and recovered through successful WMI probing.
PAN-94571	Fixed an issue on PA-800 Series, PA-3200 Series, and PA-5200 Series firewalls where tunnel-bound traffic was incorrectly routed through an ECMP route instead of a PBF route as expected.
PAN-94497	Fixed an issue where the default static route was not present in the routing table after you removed the DHCP-provided default gateway when you configured a default static route and DHCP provided the same default route.
PAN-94385	Fixed an issue on Log Collectors where the show log-collector serial-number <LC_serial_number> CLI command displayed log ages that exceeded log expiration periods.
PAN-94288	Fixed an issue where the default view and maximized view of the Application Usage report (ACC > Network Activity) didn't display matching values when you set the Time to Last 12 Hrs or a longer period.
PAN-94221	Fixed an issue when QoS was configured where the dataplane restarted due to a packet process failure.
PAN-94163	Fixed an issue on firewalls deployed in virtual wire mode where SSL decryption failed due to a memory pool allocation failure.
PAN-94058	(GlobalProtect configurations on PAN-OS 8.0.8 and later releases only) Fixed an issue where a configured Layer 3 interface erroneously opened ports 28869/tcp and 28870/tcp on the IP address assigned to that Layer 3 interface.
PAN-93973	Fixed an issue on an M-100 appliance where logging stopped when a process (<i>vldmgr</i>) stopped responding.
PAN-93937	Fixed an issue where the management server (<i>mgmtsvr</i>) process on the firewall restarted when you pushed configurations from the Panorama management server.
PAN-93847	Fixed an issue where a null-pointer exception caused the device server ("devsrv") process on the management plane to restart.

Issue ID	Description
PAN-93331	Fixed an issue where the firewall applied the wrong checksum when a re-transmitted packet in a NAT session had different TCP flags, which caused the recipient to drop those packets.
PAN-93329	Fixed an issue where the non-session-owner firewall in a high availability (HA) active/active configuration with asymmetric traffic flow dropped TCP traffic when TCP reassembly failed.
PAN-93127	Fixed an intermittent issue where NAT traffic was dropped when NAT parameters were introduced or changed in the path between the LSVPN GlobalProtect gateway and the GlobalProtect satellite. To leverage this fix in your network, you must also enable Tunnel Monitoring on the GlobalProtect Gateway ("Network > GlobalProtect > Gateways > <"gp-gateway"> > Satellite > Tunnel Settings").
PAN-92893	Fixed an issue that occurred during the reboot process and caused some firewalls to go in to maintenance mode.
PAN-92788	Fixed an issue where the PAN-OS XML API returned the same job IDs for all report jobs on the firewall. With this fix, the PAN-OS XML API returns the correct job ID for each report job.
PAN-92569	Fixed an issue where the firewall displayed a continue-and-override response page when users tried to access a URL that the firewall incorrectly categorized as unknown because it learned the URL field as an IP address.
PAN-92445	Fixed an issue where the Panorama management server didn't display log data in Monitor > Logs , the ACC tab, or reports when Panorama was in a different timezone than the Dedicated Log Collectors because Panorama applied the wrong time filter.
PAN-92033	Fixed an issue during the software download process that prevented some firewalls and appliances from properly receiving these images.
PAN-91926	Fixed an issue where GlobalProtect users could not access some websites decrypted by the firewall due to an issue with premature deletion of proxy sessions.
PAN-91361	Fixed an issue where client connections initiated with HTTP/2 failed during SSL Inbound Inspection decryption because the firewall removed the Application-Layer Protocol Negotiation (ALPN) extension within the server hello packet instead of forwarding the extension to the client.
PAN-91238	Fixed an issue where an Aggregate Ethernet (AE) interface with Link Aggregation Control Protocol (LACP) enabled on the firewall went down

Issue ID	Description
	after a cisco-nexus primary virtual port channel (vPC) switch LACP peer rebooted and came back up.
PAN-90917	Fixed an issue where IP addresses for predefined External Dynamic Lists were not displayed on the web interface.
PAN-90824	An enhancement was made to improve compatibility for the HTTP log forwarding feature so that you can specify the TLS version that the HTTP log forwarding feature uses to connect to the HTTP server. To specify the version, use the debug system https-settings tls-version CLI command. (To view the currently specified version, use the debug system https-settings command.)
PAN-90448	Fixed an issue where PA-7000 Series and PA-5200 Series firewalls didn't properly Rematch all sessions on config policy change for offloaded sessions (Device > Setup > Session).
PAN-90048	Fixed an issue where automatic commits failed after you configured Security policy rules that referenced region objects for the source or destination and then upgraded the PAN-OS software.
PAN-88829	Fixed an issue where the firewall was unable to verify a signature and marked the response as unavailable when the OCSP responder signed the response and sent it to the OCSP client but did not include the certificate.
PAN-87855	Fixed an issue where some ICMP Type 4 traffic was not blocked as expected after you created a deny Security policy rule with custom App-ID for ICMP Type 4 traffic.
PAN-87079	(PA-3060, PA-3050, PA-5000 Series, PA-5200 Series, and PA-7000 Series firewalls only) Fixed an issue where Threat logs displayed an Other IP Flood message instead of identifying the threat name of the correct protocol (such as TCPFlood) when traffic reached the configured SYN flood max-rate threshold (Objects > Security Profiles > DoS Protection > <DoS_Protection_profile> > Flood Protection > SYN Flood).
PAN-86672	Fixed a rare issue where a commit caused the disk to become full due to an incorrect disk quota-size value, which caused the firewall to behave unpredictably (for example, the web interface and CLI became unresponsive).
PAN-84836	A security-related fix was made to address a Cross-Site Scripting (XSS) vulnerability in the PAN-OS response to a GlobalProtect gateway (CVE-2018-10139).

Issue ID	Description
PAN-84647	Fixed an issue with scheduled log exports that prevented firewalls running in FIPS-CC mode from successfully exporting the logs using Secure Copy (SCP).
PAN-83946	Fixed an issue where the default QoS profile limited the available bandwidth to 10Gbps when you specifically applied the profile to the ae2 interface; this issue occurred regardless of the bandwidth setting you configured specifically for that profile.
PAN-83900	Fixed an issue where the Panorama management server did not run ACC reports or custom reports because the <i>reportd</i> process stopped responding when an administrator tried to access a device group to which that administrator did not have access.
PAN-83628	Fixed an issue where an error was displayed when filtering the threat log because the buffer was cleared before prepending the query strings to it.
PAN-83469	Fixed an issue where firewalls were unable to connect to a log collector after you modified the Log Forwarding Preferences (Panorama > Collector Groups > <group> > Device Log Forwarding).
PAN-83030	Fixed an issue where an SSL session was reset after displaying the SSL decryption opt-out page regardless whether the user chose Yes or No .
PAN-81320	Fixed an issue where administrators could perform a commit lock through the API but could not remove the lock using the same API account credentials on the web interface.
PAN-80794	A protocol-related fix was made to address a bug in the OSPF protocol.
PAN-80665	Fixed an issue in a bi-directional User-ID redistribution configuration where the User-ID (<i>userid</i>) process stopped responding when same IP address was continually associated with different usernames, which caused the IP address-to-username mapping to continually sync between firewalls.
PAN-76441	Fixed an issue where expiration of the Captive Portal browser-session cookie was incorrectly set on the browser to 24 hours by default. With this fix, the Captive Portal browser-session cookie expires when the browser session is terminated.
PAN-42036	Fixed a rare intermittent issue on PA-800 Series, PA-2000 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series, and PA-7000 Series firewalls where the firewall unexpectedly rebooted due to memory

Issue ID	Description
	page allocation failure, which generated a non-maskable interrupt (NMI) watchdog error on the serial console.

PAN-OS 8.0.11-h1 Addressed Issues

Issue ID	Description
PAN-99380	Fixed an issue where the dataplane stopped responding when a tunnel interface on the firewall received fragmented packets.
PAN-99263	Fixed an issue where NetFlow caused an invalid memory access issue which caused the pan_task process to stop responding.

PAN-OS 8.0.11 Addressed Issues

Issue ID	Description
PAN-97561	Fixed an issue where a Panorama appliance running PAN-OS 8.1.2 was unable to connect to the Logging Service.
PAN-97084	Fixed a rare issue where the task manager failed to load in the web interface when a pending job caused subsequent completed jobs to be inappropriately held in memory.
PAN-96587	Fixed an issue where PA-7000 Series and PA-5200 Series firewalls intermittently failed to forward logs to Log Collectors or the Logging Service due to DNS resolution failure for the FQDNs of those log receivers.
PAN-96490	Fixed an issue where syslog servers misrepresented HIP Match, Authentication, and User-ID logs received from the firewall because the order changed in the first seven syslog fields for those log types. With this fix, the first seven syslog fields are the same for all log types.
PAN-96150	Fixed a memory corruption error that caused the dataplane to restart when content decode length was zero.
PAN-95884	Fixed an issue where routing FIB entries that were learned from a BGP peer were not deleted when BGP Peering went down.
PAN-95740	Fixed an issue where multicast FIB entries were inconsistent across dataplanes, which caused the firewall to intermittently drop multicast packets.
PAN-95445 <i>This fix requires the VMware NSX 2.0.4 or a later plugin.</i>	Fixed an issue where VM-Series firewalls for NSX and firewalls in an NSX notify group (Panorama > VMware NSX > Notify Group) briefly dropped traffic while receiving dynamic address updates after the primary Panorama in a high availability (HA) configuration failed over.
PAN-94920	Fixed an issue where PA-5200 Series firewalls in a high availability (HA) active/active configuration experienced internal packet corruption that caused the firewalls to stop passing traffic when the active member of a cluster came back up as passive after being either suspended or rebooted (moving from tentative to passive state).
PAN-94646	Fixed an issue with firewalls in a high availability (HA) configuration where a an HA sync initiated from the active peer caused a race condition while processing the previous request.

Issue ID	Description
PAN-94586	Fixed an issue where the Panorama management server exported reports slowly or not at all due to DNS resolution failures.
PAN-94578	Fixed an issue where WildFire submissions with a filename that contained %20n or a subject that contained %n caused the management server (<i>mgmtsrvr</i>) process to stop responding.
PAN-94452	Fixed an issue where the firewall recorded GPRS Tunneling Protocol (GTP) packets multiple times in firewall-stage packet captures (PCAPs).
PAN-94450	Fixed an issue where QSFP+ interfaces (13 and 14) on a PA-7000-20GQ-NPC Network Processing Card (NPC) unexpectedly flapped when the card was booting up.
PAN-94165	Fixed an issue where the firewall used an incorrect next hop in the Border Gateway Protocol (BGP) route that it advertised to External BGP (eBGP) peers in the BGP peer group.
PAN-94122	Fixed an issue where firewalls intermittently blocked SSL traffic due to a certificate timeout error after you enabled SSL Forward Proxy decryption and selected to Block sessions on certificate status check timeout (Objects > Decryption Profile > <Decryption_profile> > SSL Decryption > SSL Forward Proxy) .
PAN-94070	Fixed an issue where Bidirectional Forwarding Detection (BFD) sessions were active in only one virtual router when two or more virtual routers had active BGP sessions (with BFD enabled) using the same peer IP address.
PAN-94023	Fixed an issue where the <code>requestsystem external-list show type ip name <EDL_name></code> CLI command did not display external dynamic list entries after you restarted the management server (<i>mgmtsrvr</i>) process.
PAN-93854	Fixed an issue where the VM-Series firewall for NSX randomly disrupted traffic due to high CPU usage by the <i>pan_task</i> process.
PAN-93754	A security-related fix was made to address vulnerabilities related to some SAML implementations (CVE-2018-0486 and CVE-2018-0489). Refer to www.kb.cert.org/vuls/id/475445 for details.
PAN-93753	Fixed an issue on PA-200 firewalls where disk space usage was constantly running high and often reaching maximum capacity. With this fix, the PA-200 firewall purges logs more quickly and it no longer requires as much space for monitor daemons.

Issue ID	Description
PAN-93722	Fixed an issue where the firewall failed to perform decryption because endpoints tried to resume decrypted inbound perfect forward secrecy (PFS) sessions.
PAN-93687	Fixed an issue where the firewall dataplane restarted, disrupting traffic, because the <i>all_pktproc</i> process stopped responding when the firewall decoded HTTP message bodies with chunked transfer encoding or gzip-compressed data.
PAN-93609	Fixed an issue where the firewall silently dropped the first packet of a session when that packet was received as a fragmented packet (typically with UDP traffic).
PAN-93431	Fixed an issue where the Panorama management server failed to export Traffic logs as a CSV file (Monitor > Logs > Traffic) after you set the Max Rows in CSV Export to more than 500,000 rows (Panorama > Setup > Management > Logging and Reporting Settings > Log Export and Reporting).
PAN-93411	Fixed an issue on VM-Series firewalls for KVM where applications that relied on multicasting failed because the firewalls filtered multicast traffic by the physical function (PF) after you configured them to use single root I/O virtualization (SR-IOV) virtual function (VF) devices.
PAN-93318	Fixed an issue where firewall CPU usage reached 100 per cent due to SNMP polling for logical interfaces based on updates to the Link Layer Discovery Protocol (LLDP) MIB (LLDP-V2-MIB.my).
PAN-93254	Fixed an issue where automatic threat packet captures on the firewall displayed a "File not found" error when attempting to retrieve these captures from a threat log entry.
PAN-93242	A security-related fix was made to prevent a Cross-Site Scripting (XSS) vulnerability in a PAN-OS web interface administration page (CVE-2018-9337).
PAN-92958	Fixed an issue where disk utilization increased unnecessarily because the firewall did not archive and rotate the <i>/var/on</i> file, which therefore grew to over 40MB.
PAN-92944	Fixed an issue where the firewall assigned the wrong URL filtering category to traffic that contained a malformed host header. With this fix, the firewall enables the blocking of any traffic with a malformed URL.
PAN-92738	Fixed an issue on the Panorama management server where administrators with read-only privileges could not view deployment

Issue ID	Description
	Schedules for content updates (Panorama > Device Deployment > Dynamic Updates).
PAN-92481	Fixed an issue where the root partition became full. With this fix, the /tmp/tplsp_to_validate.xml file and the /tmp/panorama_pushed folder are moved to the /opt/pancfg/mgmt/tmp folder.
PAN-92456	Fixed an issue on the Panorama management server where administrators couldn't log in to the web interface because disk space utilization reached 100 per cent due to the continuous growth of cmserror log files.
PAN-92366	Fixed an issue where PA-5200 Series firewalls in an active/passive high availability (HA) configuration dropped Bidirectional Forwarding Detection (BFD) sessions when the passive firewall was in an initialization state after you rebooted it.
PAN-92257	Fixed an issue where the firewall was intermittently sending incorrect bytes-per-packet values for some flows to the NetFlow collector.
PAN-92163	Fixed an issue where firewalls in an active/passive high availability (HA) configuration took longer than expected to fail over after you configured them to redistribute routes between an Interior Gateway Protocol (IGP) and Border Gateway Protocol (BGP).
PAN-91785	Fixed an issue where the firewall intermittently did not apply antivirus exceptions after you added more than one in an Antivirus profile (Objects > Security Profiles > Antivirus > <Antivirus_profile> > Virus Exception).
PAN-91662	Fixed an issue where a certificate was loaded without a digital signature, which caused the configuration daemon (<i>configd</i>) to stop responding.
PAN-91503	Fixed an issue where the firewall failed to generate tech support logs because there was not enough disk space available.
PAN-91370	Fixed an issue where the firewall dropped IPv6 traffic while enforcing IPv6 bidirectional NAT policy rules because the firewall incorrectly translated the destination address for a host that resided on a directly attached network.
PAN-91254	Fixed an issue where end user accounts were locked out after you configured authentication based on a RADIUS server profile with multiple servers (Device > Server Profiles > RADIUS) and enabled the gateway to Retrieve Framed-IP-Address attribute from authentication

Issue ID	Description
	server (Network > GlobalProtect > Gateways > <gateway> > Agent > Client Settings > <clients_configuration> > IP Pools). With this fix, instead of requesting framed IP addresses from all the servers in a RADIUS server profile at the same time, the firewall sends the request to only one server at a time until one of the servers responds.
PAN-91095	Fixed an issue where the firewall did not perform a validation check when you set the Subnet Mask while configuring the firewall as a DHCP server (Network > DHCP > <interface> > Options).
PAN-90952	Fixed an issue on PA-5000 Series firewalls where multicast traffic failed because PAN-OS did not remove stale sessions from the hardware session offload processor.
PAN-90835	A security-related fix was made to prevent a Cross-Site Scripting (XSS) attack through the URL Continue page (CVE-2018-7636).
PAN-90535	Fixed an issue where the firewall unnecessarily sent an Authorize-only request to the RADIUS server which was denied during the login process if you disabled the Retrieve Framed-IP-Address attribute from authentication server (Network > GlobalProtect > Gateways > <gateway> > Agent > Client Settings > <clients_configuration> > IP Pools) in the GlobalProtect gateway configuration.
PAN-90531	Fixed an issue where the firewall discarded any unsaved changes you made to the exceptions in a Vulnerability Protection profile after you enabled or disabled (cleared) the Show all signatures option (Objects > Security Profiles > Vulnerability Protect > <Vulnerability_Protection_profile> > Exceptions).
PAN-90418	Fixed an issue where PA-7000 Series, PA-5200 Series, PA-5000 Series, PA-3200 Series, and PA-3000 Series firewalls dropped packets because their dataplanes restarted due to QoS queue corruption.
PAN-89525	Fixed a configuration parsing issue where a default setup of the Authentication Profile caused the firewall to reboot during commit. If the administrator configured the Authentication Profile with any allowed values, including the default values, the configuration committed successfully. The issue was observed on a PA-500 firewall in FIPS-CC mode.
PAN-89177	Fixed an issue where the Panorama management server ran out of disk space because PAN-OS did not automatically purge configuration export files from the tmp folder after exporting them.
PAN-89164	Fixed an issue where content update failures (associated with the “Content update job failed for user Auto update agent” error message)

Issue ID	Description
	had only a high severity level in System logs. With this fix, content update failures have a critical severity level for better visibility.
PAN-88897	Fixed an issue where SNMP managers could not retrieve firewall power supply information associated with the <code>entPhysicalEntry</code> (1.3.6.1.2.1.47.1.1.1) and <code>entPhysicalDescr</code> (1.3.6.1.2.1.47.1.1.1.1) SNMP objects.
PAN-88473	Fixed an issue where the firewall was sending incorrect bytes-per-packet values to the NetFlow collector when two servers were configured in the same NetFlow profile.
PAN-87166	Fixed a rare issue on PA-7000 Series firewalls where 20GQ NPC QSFP+ ports didn't link up (during online insertion and removal (OIR), link-state change, or boot up events) and became unrecoverable until the NPC was restarted.
PAN-86934	Fixed an issue where the firewall applied case sensitivity to the names of shared user groups that were defined in its local database and, as a result, users who belonged to those groups couldn't access applications through GlobalProtect Clientless VPN even after successful authentication. With this fix, the firewall ignores character case when evaluating the names of user groups in its local database.
PAN-86028	Fixed an issue in an HA active/active configuration where traffic in a GlobalProtect VPN tunnel in SSL mode failed after Layer 7 processing when asymmetric routing was involved.
PAN-85773	Fixed an issue where, after end users resumed their sessions, GlobalProtect connections failed with a client certificate error because the certificate host ID field was not cached in the session cache.
PAN-82502	Fixed an issue where the firewall web interface did not display the task manager when indices were corrupted and did not purge the old jobs as expected.
PAN-80922	Fixed an issue where the firewall failed to parse the merged configuration file after you changed the master key; it parsed only the running configuration file. With this fix, the firewall parses both files as expected after you change the master key.
PAN-80091	Fixed an issue where no results were returned for a Global Find request when using the short name <code>domain\group</code> format.
PAN-79786	Fixed an issue where Panorama was unable to pull any groups from a specific domain when the query for users included a domain name that ended with a backslash (<code>"\"</code>) character.

Issue ID	Description
PAN-79450	Fixed an issue where all WildFire jobs on the firewall were stuck at zero percent progress, which prevented the firewall from installing the latest WildFire updates.

PAN-OS 8.0.10 Addressed Issues

Issue ID	Description
WF500-4625	Fixed an issue where the WF-500 appliance provided no option to configure the master key. With this fix, you can use the request master-key new-master-key <key> lifetime <lifetime> CLI command to configure the master key.
WF500-4363	Fixed an issue where firewalls and Panorama management servers could not retrieve reports from a WF-500 appliance due to an interruption in its data migration after you upgraded the appliance from a PAN-OS 7.1 release to a PAN-OS 8.0 or later release. With this fix, you can run the new debug device data-migration status CLI command on the WF-500 appliance after each upgrade to verify data migration finished successfully (output is Migration inMySQL is successfu l). Don't perform additional upgrades on the WF-500 appliance until the data migration finishes.
PAN-95504	Fixed an issue on the firewall and Panorama management server where the web interface became unresponsive because the management server process (<i>mgmtsrvr</i>) restarted after you set its debugging level to debug (through the debug management-server on debug CLI command).
PAN-95197	Fixed an issue where mobile endpoints that used GPRS Tunneling Protocol (GTP) lost traffic and had to reconnect because the firewall dropped the response message that a Gateway GPRS support node (GGSN) sent for a second Packet Data Protocol (PDP) context update.
PAN-94912	Fixed an issue where PA-5200 Series and PA-3200 Series firewalls in an active/active HA configuration sent packets in the wrong direction in a virtual wire deployment.
PAN-94853	Fixed an issue where mobile endpoints that use GPRS Tunneling Protocol (GTP) lose GTP-U traffic because the firewall dropped all GTP-U packets as packets without sessions after receiving two GTP requests with the same tunnel endpoint identifiers (TEIDs) and IP addresses.
PAN-94379	Fixed an issue in a Panorama deployment with a Collector Group containing multiple Log Collectors where the logging search engine restarted after you changed the SSH keys used for HA. The disruption to the search engine caused an out-of-memory condition and caused Panorama to display logs and report data from only one Log Collector in the Collector Group.

Issue ID	Description
PAN-94167	Fixed an issue where a firewall forwarded a deleted or expired IP address-to-username mapping to another firewall through User-ID Redistribution but the receiving firewall still displayed the mapping as an active IP address-to-username mapping.
PAN-93839	Fixed an issue where administrators failed to log in to the firewall due to an out-of-memory condition that intermittently caused the firewall to continuously restart processes. (PAN-90143 provided an initial memory enhancement in PAN-OS 8.0.9 that reduced the frequency of these out-of-memory events.)
PAN-93715	In certain customer environments, enhancements in PAN-OS 8.0.10 to change fan speeds may help reduce rare cases of drive communication failure in PA-5200 Series firewalls.
PAN-93522	Fixed an issue on firewalls in an HA configuration where traffic was disrupted because the dataplane restarted unexpectedly when the firewall concurrently processed HA messages and packets for the same session. This issue occurred on all firewall models except the PA-200 and VM-50 firewalls.
PAN-93336	Fixed an issue where the firewall intermittently became unresponsive because the management server process (<i>mgmtsvr</i>) stopped responding during a commit after you configured policy rules to use external dynamic lists (EDLs).
PAN-93244	A security-related fix was made to prevent a Cross-Site Scripting (XSS) attack through the PAN-OS session browser (CVE-2018-9335).
PAN-93234	Fixed an issue where a Panorama management server running PAN-OS 8.0 could not switch Context to a firewall running PAN-OS 7.1 or an earlier release.
PAN-93233	Fixed an issue where PA-7000 Series firewalls caused slow traffic over IPSec VPN tunnels because the firewalls reordered TCP segments during IPSec encryption when the tunnel session and inner traffic session were on different dataplanes.
PAN-93089	A security-related fix was made to prevent denial of service (DoS) to the management web interface (CVE-2018-8715).
PAN-93052	Fixed an issue where IPv6 BGP peering persisted (not all BGP routes were withdrawn) after the associated firewall interface went down.

Issue ID	Description
PAN-92789	Fixed an issue where VM-Series firewalls deleted logs by reinitializing the logging disk when the periodic file system integrity check (FSCK) took over 30 minutes during bootstrap.
PAN-92725	Fixed an issue on the firewall and Panorama management server where the web interface became unresponsive because the <i>cord</i> process restarted after you configured multiple log forwarding destinations in a single forwarding rule for Correlation logs (Device > Log Settings).
PAN-92678	Fixed an issue on Panorama management servers in an HA configuration where, after failover caused the secondary HA peer to become active, it failed to deploy scheduled dynamic updates to Log Collectors and firewalls.
PAN-92487	<p>Fixed an issue where enabling jumbo frames (Device > Setup > Session) reduced throughput because:</p> <ul style="list-style-type: none"> • The firewalls hardcoded the maximum segment size (TCP MSS) within TCP SYN packets and in server-to-client traffic at 1,460 bytes when packets exceed that size. With this fix, the firewalls no longer hardcode the TCP MSS value for TCP sessions. • PA-7000 Series and PA-5200 Series firewalls hardcoded the maximum transmission unit (MTU) at 1,500 bytes for the encapsulation stage when tunneled clear-text traffic and the originating tunnel session were on different dataplanes. With this fix, the firewalls use the MTU configured for the interface (Network > Interfaces > <interface> > Advanced > Other Info) instead of hardcoding the MTU at 1,500 bytes.
PAN-92251	Fixed an issue where VM-Series firewalls used the incorrect MAC address in DHCP messages initiated from a subinterface after you configured that subinterface as a DHCP Client (Network > Interfaces > Ethernet > <subinterface> > IPv4) and disabled the Use Hypervisor Assigned MAC Address option (Device > Management > Setup > General Settings).
PAN-92152	Fixed an issue where the firewall web interface displayed a blank Device > Licenses page when you had 10 x 5 phone support with empty feature.
PAN-92082	Fixed an issue where the firewall didn't generate URL Filtering logs for user credential submissions associated with a URL that was not a container page after you selected Log container page only and set the User Credential Submission action to alert for the URL category in a URL Filtering profile (Objects > Security Profiles > URL Filtering > <ULR_Filtering_profile>). With this fix, the firewall generates URL

Issue ID	Description
	Filtering logs for user credential submissions regardless of whether you enable Log container page only in the URL Filtering profile.
PAN-92017	Fixed an issue where Log Collectors that belonged to a collector group with a space in its name failed to fully connect to one another, which affected log visibility and logging performance.
PAN-91591	Fixed an issue where the Globalprotect agent failed to establish a TCP connection with the Globalprotect gateway when TCP SYN packets had unsupported congestion notification flag bits set (ECN or CWR).
PAN-91429	Fixed an issue where PA-5200 Series firewalls rebooted when you ran the set ssh service-restart mgmt CLI command multiple times.
PAN-91360	Fixed an issue where, in rare cases, the firewall couldn't establish connections with GlobalProtect agents because the <i>rasmgr</i> process stopped responding when hundreds of end users logged in and out of GlobalProtect at the same time.
PAN-91194	Fixed an issue where a firewall dataplane running with high CPU utilization became unstable and the <i>all_pktproc</i> process stopped responding when the firewall processed a high rate of IP addresses with unknown usernames for User-ID mappings.
PAN-91098	Fixed an issue in Layer 2 deployments where using ECDHE ciphers for SSL Inbound Inspection decryption caused sessions to become stuck and ultimately time out.
PAN-91088	Fixed an issue on PA-7000 Series firewalls in an HA configuration where the HA3 link did not come up after you upgraded to PAN-OS 8.0.6 or a later 8.0 release.
PAN-90959	Fixed an issue where PA-5200 Series firewalls dropped offloaded sessions after you selected to Enforce Symmetric Return in a Policy Based Forwarding (PBF) policy rule (Policies > Policy Based Forwarding > <PBF_rule> > Forwarding).
PAN-90954	A security-related fix was made to prevent a local privilege escalation vulnerability that could potentially result in the deletion of files (CVE-2018-9242).
PAN-90920	Fixed an issue on PA-5200 Series firewalls where the dataplane restarted due to an internal path monitoring failure.
PAN-90890	Fixed an issue where the User-ID process (<i>userid</i>) stopped responding when a virtual system connected to more than one User-ID agent with NT LAN Manager (NTLM) enabled.

Issue ID	Description
PAN-90842	Fixed an issue where commits failed after you changed the default Size Limit to a custom value for MacOSX files that the firewall forwarded to WildFire (Device > Setup > WildFire).
PAN-90692	Fixed an issue where PA-5200 Series firewalls dropped offloaded traffic after you enabled session offloading (enabled by default), configured subinterfaces on the second aggregate Ethernet (AE) interface group (ae2), and configured QoS on a non-AE interface.
PAN-90689	Fixed an issue where firewalls in an active/active HA configuration dropped packets in IPSec tunnel traffic because the secondary firewall didn't update the Encapsulating Security Payload (ESP) sequence number during failover.
PAN-90688	Fixed an issue where end users could not access applications through GlobalProtect Clientless VPN when the application server used cookie-based session persistence through HTML metadata.
PAN-90623	Fixed an issue where the Panorama management server displayed template configurations as Out of Sync for firewalls with multiple virtual systems even though the template configurations were in sync.
PAN-90514	Fixed an issue on firewalls in an active/active HA configuration where the secondary firewall dropped ping and SSH sessions on its virtual wire interfaces when the primary firewall was the session owner.
PAN-90509	Fixed an issue where end users could not access applications through GlobalProtect Clientless VPN because the firewall failed to respond correctly to a client certificate request from the application server.
PAN-90462	Fixed an issue on the Panorama management server where System logs displayed null as the client IP address for the log forwarding connections of PA-7000 Series firewalls that forwarded logs to Panorama.
PAN-90371	Fixed an issue where the firewall didn't record an IP address-to-username mapping for a user who successfully logged in to the GlobalProtect gateway.
PAN-90337	Fixed an issue where Panorama Log Collectors stopped forwarding URL Filtering logs over TCP to a syslog server after failing to create the required last-candidatecfg.xml file.
PAN-90291	Fixed an issue on Panorama virtual appliances in Panorama mode that were deployed in an HA configuration with local Log Collectors in a single Collector Group, where HA failover caused the logging search engine to stop functioning. This issue prevented the secondary HA

Issue ID	Description
	peer from displaying existing logs or receiving new logs until the search engine recovered.
PAN-90290	Fixed an issue on the Panorama management server where commits failed with schema validation errors.
PAN-89998	Fixed an issue where the Panorama management server stopped receiving new logs from firewalls because delayed log purging caused log storage on the Log Collectors to reach maximum capacity.
PAN-89992	Fixed an issue where the firewall did not efficiently handle traffic in which the number of Address Resolution Protocol (ARP) packets exceeded the processing capacity of the firewall. With this fix, the firewall handles ARP packets more efficiently.
PAN-89461	Fixed an issue where accessing websites that had normal gzip content-encoding generated multi-level encoding errors.
PAN-89353	Fixed an issue where stale IP address-to-username mappings in the User-ID cache intermittently prevented the firewall from refreshing the mappings or creating new ones.
PAN-89162	Fixed an issue where commits and content update installations failed due to memory allocation errors.
PAN-88908	Fixed an issue where the Panorama management server generated custom reports in which the number of lines exceeded what you specified in the report configuration (Monitor > Manage Custom Reports).
PAN-88880	Fixed an issue where client browsers stopped responding after downloading a file that triggered a Security policy rule with a File Blocking profile in which the Action was continue (Objects > Security Profiles > FileBlocking) .
PAN-88852	Fixed an issue where VM-Series firewalls stopped displaying URL Filtering logs after you configured a URL Filtering profile with an alert action (Objects > Security Profiles > URL Filtering).
PAN-88752	Fixed an issue where User-ID agents configured to detect credential phishing did not detect passwords that contained a blank space.
PAN-88388	Fixed an issue where you could not export certificates when you accessed the firewall web interface through a browser that ran Firefox v56 or later or ran Chrome v66 or later (Device > Certificate Management > Certificates > Device Certificates).

Issue ID	Description
PAN-88200	Fixed an issue where firewalls with multiple virtual systems did not import EDLs that you assigned to policy rules.
PAN-87964	Fixed an issue where the firewall couldn't render URL content for end users after you configured GlobalProtect Clientless VPN with a Hostname set to a Layer 3 subinterface or VLAN interface (Network > GlobalProtect > Portals > <portal> > Clientless VPN > General).
PAN-87926	Fixed an issue where commit operations took longer than expected to finish on firewalls that had over 100 policy rules that referenced tens of thousands of IP addresses.
PAN-87552	Fixed an issue where commit validation failed on firewalls after you disabled the option to Share Unused Address and Service Objects with Devices on the Panorama management server, assigned the firewalls to a template stack, and pushed an interface configuration that referenced an address object instead of an address that you typed.
PAN-87520	Fixed an issue where the Cross-Origin Resource Sharing (CORS) policy on the firewall allowed requests from other domains to interact with the firewall through PAN-OS XML API requests and read responses. With this fix, the CORS policy is disabled on the firewall.
PAN-87265	Fixed an issue where the Panorama management server displayed no output for the User Activity Report (Monitor > PDF Reports > User Activity Report).
PAN-86647	Fixed an issue on the Panorama management server where editing the Description of a shared policy rule and clicking OK caused the Target setting to revert to Any firewalls instead of the selected firewalls.
PAN-86630	Fixed an issue where the firewall dropped H.323 gatekeeper-assisted calls after failing to perform NAT translation of third-party addresses in H.323 messages.
PAN-85206	Fixed an issue where VM-Series firewalls for NSX did not forward files to the WildFire cloud for analysis.
PAN-83890	Fixed an issue on the Panorama management server where you could not preview configuration changes after you switched Context to a firewall, added an administrative account to the firewall, and then clicked Commit and Preview Changes .
PAN-83361	Fixed an issue where Panorama Log Collectors did not receive firewall logs due to incorrect permissions after you upgraded the Panorama software.

Issue ID	Description
PAN-82942	Fixed an issue where the firewall rebooted because the User-ID process (<i>userid</i>) restarted several times when endpoints, while requesting services that could not process HTTP 302 responses (such as Microsoft update services), authenticated to Captive Portal through NT LAN Manager (NTLM) and immediately disconnected.
PAN-81751	Fixed an issue where the firewall displayed the following error when you tried to log in to the web interface after a report job took a configuration lock: <code>Timeout while getting config lock. Please try again.</code>
PAN-81588	Fixed an issue where the ciphers you specified for access to the firewall management (MGT) interface didn't work after a PAN-OS upgrade because the <code>sshd_config</code> file containing the SSH running configuration became blank.
PAN-81382	Fixed an issue where the firewall took longer than expected to collect group mapping information from Active Directory groups that had circular nesting (Device > User Identification > Group Mapping Settings > <group_mapping_configuration> > Group Include List).
PAN-80664	Fixed an issue where the firewall generalizes messages received from back-end authentication servers instead of displaying the messages without modification.
PAN-79695	Fixed an issue on PA-7000 Series, PA-5200 Series, and PA-5000 Series firewalls where the clear session all filter CLI command cleared sessions only on <code>dp1</code> when that dataplane was the session owner instead of clearing sessions on all dataplanes. With this fix, the command clears sessions on all dataplanes regardless of which is the session owner.
PAN-79317	Fixed an issue where the firewall failed to prepare a USB flash drive for bootstrapping when the drive had 8GB or more memory.
PAN-79071	Fixed an issue where loading a partial configuration (using the load config partial CLI command) changed the port numbers in service and service group objects.
PAN-78046	Fixed an issue where only administrators with the predefined superuser role could specify the Number of Bits and Digest algorithm when generating a certificate to be Signed By an External Authority (CSR) (Device > Certificate Management > Certificates).

Issue ID	Description
PAN-77229	Fixed an issue on firewalls with SSL Forward Proxy decryption enabled where the dataplane restarted due to an out-of-memory condition after you performed multiple commits.
PAN-71902	Fixed an issue where, after you used a configuration mode CLI command to create a zone without specifying the interface type (set zone <zone_name> network), the firewall web interface displayed the type as layer3 (Network > Zones), which gave the misleading impression that the zone configuration was complete.

PAN-OS 8.0.9 Addressed Issues

Issue ID	Description
WF500-4599	Fixed an issue on WF-500 appliance clusters where attempts to submit samples for analysis through the WildFire XML API failed with a 499 or 502 error in the HTTP response when the local worker was fully loaded.
WF500-4535	Fixed an issue where the WF-500 appliance could not forward logs over TCP or SSL to a syslog server.
WF500-4473	Fixed an issue where the root partition on the WF-500 appliance reached its maximum storage capacity because the following log files had no size limit and grew continuously: appweb_access.log, trap-access.log, wpc_build_detail.log, rsyncd.log, cluster-mgr.log, and cluster-script.log. With this fix, the appweb_access.log, trap-access.log, and wpc_build_detail.log logs have a limit of 10MB and the WF-500 appliance maintains one rotating backup file for each of these logs to store old data when a log exceeds the limit. Also with this fix, the rsyncd.log, cluster-mgr.log, and cluster-script.log logs have a limit of 5MB and the WF-500 appliance maintains eight rotating backup files for each of these logs.
WF500-4472	Fixed an issue where the WF-500 appliance restarted because the virtual memory limit was too small for the management server (mgmtsvr) process. With this fix, mgmtsvr has a higher virtual memory limit.
WF500-4190	Fixed an issue on WF-500 appliances where the show cluster all-peers CLI command displayed <code>siggen-db:Ready</code> (signature generation database ready) for worker nodes in a WildFire cluster even though worker nodes don't generate signatures. With this fix, the command displays <code>siggen-db:Stopped</code> for worker nodes.
PAN-94845	Fixed an issue where App-ID did not recognize GPRS Tunneling Protocol User Plane (GTP-U) in GTP messages on port 2152 when only single-direction message packets arrived (Traffic logs indicated <code>application insufficient-data</code>).
PAN-94386	Fixed an issue where the firewall dropped packet data protocol (PDP) context update and delete messages that had a tunnel endpoint identifier (TEID) of zero in GPRS Tunneling Protocol (GTP) traffic, and the traffic failed when the dropped messages were valid.
PAN-94170	Fixed an issue where GPRS Tunneling Protocol (GTP) traffic failed because the firewall dropped GTP-U echo request packets.

Issue ID	Description
PAN-93106	Fixed an issue where the Google Chrome browser displayed certificate warnings for self-signed ECDSA certificates that you generated on the firewall.
PAN-92916	Fixed an issue where firewalls configured for User-ID redistribution failed to redistribute IP address-to-username mappings due to a memory leak.
PAN-92604	Fixed an issue where a Panorama Collector Group did not forward logs to some external servers after you configured multiple server profiles (Panorama > Collector Groups > <Collector_Group> > Collector Log Forwarding).
PAN-92564	Fixed an issue where a small percentage of writable third-party SFP transceivers (not purchased from Palo Alto Networks®) stopped working or experienced other issues after you upgraded the firewall to which the SFPs are connected to PAN-OS 8.0.8 or an earlier 8.0 release. With this fix, you must not reboot the firewall after you download and install the PAN-OS 8.0 base image until after you download and install the PAN-OS 8.0.9 release. For additional details, upgrade considerations, and instructions for upgrading your firewalls, refer to the PAN-OS 8.0 upgrade information .
PAN-92560	Fixed an issue where SSL Forward Proxy decryption did not work after you excluded every predefined Hostname from decryption (Device > Certificate Management > SSL Decryption Exclusion).
PAN-92268	Fixed an issue on PA-7000 Series and PA-5200 Series firewalls where one or more dataplanes did not pass traffic when you ran several operational commands (from any firewall user interface or from the Panorama management server) while committing changes to device or network settings or while installing a content update.
PAN-92254	Fixed an issue on PA-7000 Series firewalls with 20GXM Magnum NPC cards where commits failed when the firewall configuration was large. With this fix, the 20GXM Magnum NPC cards have a larger internal configuration memory allocator and CTD memory buffer.
PAN-92170	Fixed an issue on VM-500 and VM-700 firewalls where you could not configure connections to more than 400 Terminal Services (TS) agents even though those firewall models were designed to support up to 1,000 TS agent connections.
PAN-91776	Fixed an issue where end users could not authenticate to GlobalProtect when you specified a User Domain with Microsoft-supported symbols such as the dollar symbol (\$) in the authentication profile (Device > Authentication Profile).

Issue ID	Description
PAN-91774	Fixed an issue on Panorama management servers in an HA configuration where the primary peer did not synchronize template changes to the secondary peer.
PAN-91689	Fixed an issue where the Panorama management server removed address objects and, in the Network tab settings and NAT policy rules, used the associated IP address values without reference to the address objects before pushing configurations to firewalls.
PAN-91564	A security-related fix was made to prevent a local privilege escalation vulnerability that allowed administrators to access the password hashes of local users (CVE-2018-9334).
PAN-91559	Fixed an issue where PA-5200 Series firewalls caused slow traffic over IPSec VPN tunnels because the firewalls reordered TCP segments during IPSec encryption.
PAN-91452	Fixed an issue where end users could not access applications through GlobalProtect Clientless VPN when the HTTP responses had both Transfer-Encoding and Content-Length headers.
PAN-91113	Fixed an issue where the <i>mrelay</i> process stopped responding when processing IPv6 neighbor discovery updates.
PAN-90970	Fixed an issue on the Panorama management server where a policy rule dialog automatically closed within a couple of seconds after you opened it to create or edit a rule.
PAN-90956	Fixed an issue where the firewall did not forward Correlation logs to syslog servers over UDP.
PAN-90899	Fixed an issue on Panorama management servers in an HA configuration where a firewall did not resume forwarding logs to the Log Collector on the passive Panorama peer after disconnecting and reconnecting to that peer.
PAN-90858	Fixed an issue on the Panorama management server where, after you clicked Send Test Log to verify that an external web server could receive firewall logs (Panorama > Server Profiles > HTTP > <HTTP_server_profile> > Payload Format), the <i>configd</i> process restarted and the Panorama user interfaces became unresponsive until the process finished restarting.
PAN-90755	Fixed an issue on firewalls in an HA configuration where endpoints did not decapsulate VPN tunnel traffic after HA failover and had to reconnect to the GlobalProtect gateway.

Issue ID	Description
PAN-90753	Fixed an issue where firewalls in an active/passive HA configuration did not synchronize multicast sessions between the firewall HA peers.
PAN-90683	Fixed an issue on PA-5200 Series firewalls in an active/passive HA configuration where the passive firewall displayed 10Gbps copper interfaces (ethernet1/1 to ethernet1/4) as up even when the connecting device (such as a switch) indicated the interfaces were down.
PAN-90622	Fixed an issue where accessing websites took longer than expected when the firewall applied SSL Inbound Inspection decryption to the websites and used CRL or OCSP to verify the status of certificates.
PAN-90565	Fixed an issue where the firewall did not accept wildcards (*) as standalone characters to match all IMSI identifiers when you configured IMSI Filtering in a GTP Protection profile (Objects > Security Profiles > GTP Protection).
PAN-90411	Fixed an issue where PA-5200 Series firewalls did not forward buffered logs to Panorama Log Collectors after connectivity between the firewalls and Log Collectors was disrupted and then restored.
PAN-90301	Fixed an issue where the firewall generated false positives during GTP-in-GTP checks because it detected some DNS-in-GTP packets as GTP-in-GTP packets (Objects > Security Profiles > GTP Protection > <GTP_Protection_profile> > GTP Inspection > GTP-U).
PAN-90143	Enhanced memory usage to reduce the frequency of out-of-memory events that intermittently caused the firewall to continuously restart processes, which prevented administrators from logging in to the firewall. PAN-93839 provides the complete and final fix for this out-of-memory condition in PAN-OS 8.0.10.
PAN-90096	Fixed an issue where Threat logs recorded incorrect IMSI values for GTP packets when you enabled Packet Capture in Vulnerability Protection profiles (Objects > Security Profiles > Vulnerability Protection > <Vulnerability_Protection_profile> > Rules).
PAN-89471	Fixed an issue where firewalls rebooted because the <i>userid</i> process restarted too often due to a socket binding failure that caused a memory leak.
PAN-89175	Fixed an issue where a firewall acting as an endpoint of an IPSec VPN tunnel dropped Encapsulating Security Payload (ESP) packets received on the old IPSec security association (SA) after rekeying and before receiving a delete message for the old IPSec SA. With this fix, the

Issue ID	Description
	firewall retains the old IPSec SA for 30 seconds while waiting for a delete message from the tunnel peer.
PAN-89171	Fixed an issue on firewalls in an HA configuration where an auto-commit failed (the error message was <code>Error:Duplicate user name</code>) after you connected a new suspended-secondary peer to an active-primary peer.
PAN-89030	Fixed an issue where the firewall could not authenticate to a hardware security module (HSM) partition when the partition password contained special characters.
PAN-88999	Fixed an issue where the Panorama management server did not return values based on the match criteria you configured in dynamic address groups (Objects > Address Groups).
PAN-88930	Fixed an issue where Threat logs and WildFire Submissions logs were not consistent with each other in terms of indicating whether the firewall blocked a file that had multiple threat identifiers. With this fix, the firewall ensures the logs are consistent by forwarding only one threat identifier for each file that it sends to WildFire.
PAN-88904	Fixed an issue where, after you disabled session offloading (using the set session offload no CLI command), flapping occurred for sessions that completed Layer 7 inspection.
PAN-88879	Fixed an issue where the firewall flooded the logrcvr.log file with the following error message: <code>Errorreading the log record from logdb, Last read seqno: 0</code> .
PAN-88760	Fixed an issue where firewalls in an HA configuration stayed in a non-functional state after a dataplane restart because they did not boot up properly.
PAN-88665	Fixed an issue where SSL connections failed because the firewall did not properly initialize certificates during a reboot.
PAN-88547	Fixed an issue where the firewall did not accept AS:0 as a value in the Set Community list of a BGP redistribution profile (Network > Virtual Routers > <router> > BGP > Redist Rules).
PAN-88537	Fixed an issue where the Panorama management server displayed commit errors and failed to push configurations to firewalls when the configurations included an Anti-Spyware security profile that contained a threat exception (Objects > Security Profiles > Anti-Spyware > <Anti-Spyware_profile> > Exceptions).

Issue ID	Description
PAN-88535	Fixed an issue on the Panorama management server where the exported device state for a firewall contained a GTP Protection profile even though the firewall did not support GPRS Tunneling Protocol (GTP). After importing the device state into the firewall, commit operations failed on the firewall.
PAN-88487	Fixed an issue where the firewall stopped enforcing policy after you manually refreshed an external dynamic list (EDL) that had an invalid IP address or that resided on an unreachable web server.
PAN-88459	Fixed an issue where the firewall returned an empty response for the PAN-OS XML API call used to display the number of IP address-to-username mappings.
PAN-88229	Fixed an issue where the firewall rebooted because the <i>dnsproxy</i> process restarted multiple times.
PAN-88159	Fixed an issue on PA-5200 Series firewalls in an active/active HA configuration where traffic latency was higher than expected because PAN-OS intermittently looped OSPF, PIM, and IGMP packets between the HA peers.
PAN-88104	Fixed an issue on the Panorama management server where, after you cloned an object or policy rule, the user interfaces became unresponsive and displayed an error when you attempted to log back in.
PAN-87990	Fixed an issue where the WF-500 appliance became inaccessible over SSH and became stuck in a boot loop after you upgraded from a release lower than PAN-OS 8.0.1 to PAN-OS 8.0.5 or a later release.
PAN-87783	Fixed an issue where a custom report configuration did not display the Description value after you configured the report, closed it, and reopened it (Monitor > Manage Custom Reports > <custom_report>).
PAN-87655	Fixed an issue where clicking the refresh button in the Monitor > Session Browser page cleared the filters you configured.
PAN-87303	Fixed an issue where the Panorama management server displayed WF-500 appliances in the list of devices that were available to Install Panorama M-Series software updates (Panorama > Device Deployment > Software) .
PAN-87271	Fixed an issue in Large-Scale VPN (LSVPN) deployments where the firewall used incorrect traffic routes because it did not flush routes learned from GlobalProtect Satellites from the routing table in a GlobalProtect gateway after you disabled the Accept published routes

Issue ID	Description
	option (Network > GlobalProtect > Gateways > <gateway> > Satellite > Route Filter).
PAN-86936	Fixed an issue on Panorama Log collectors where logs were temporarily unavailable because the <i>vldmgr</i> process restarted.
PAN-86873	Fixed an issue where the firewall advertised the OSPF not-so-stubby area (NSSA) link-state advertisement (LSA) type 7 default route to NSSA neighbors even when the OSPF backbone area was down.
PAN-86164	Fixed an issue where the PA-220 firewall intermittently performed slower than expected when processing heavy traffic. With this fix, the <i>comm</i> , <i>dha</i> , <i>tund</i> , and <i>mprelay</i> processes have improved performance.
PAN-85919	Fixed an issue where you could not select check boxes in the firewall web interface when using the Safari v11 browser.
PAN-85633	Fixed an issue on firewalls with IPv6 routing enabled where the firewalls routed traffic to a single subnetwork instead of multiple subnetworks when the same link-local IP address was used as a next hop for routing in multiple IPv6 subnetworks over a tagged Layer 3 interface (Network > Interfaces > Ethernet/VLAN > <interface> > IPV6).
PAN-85393	Fixed an issue where the Panorama management server displayed a File not found error after you tried to download a threat PCAP file when Panorama and Dedicated Log Collectors were in different timezones.
PAN-84885	Fixed an issue where configuring more than one EDL caused a memory leak in the device-server (<i>devsvr</i>) process.
PAN-84879	Fixed an issue on the Panorama management server where the ACC > Threat Activity report displayed the Others threat count as zero instead of the actual value.
PAN-83894	Fixed an issue on firewalls with multiple virtual systems where setting the Virtual System to All in the ACC tab enabled a virtual system administrator to see zones in all virtual systems instead of just the zones in the virtual system for which the administrator had the required role privileges.
PAN-83879	Fixed an issue on the Panorama management server where the debug log-collector log-collection-stats show incoming-logs CLI command did not display the correct log forwarding statistics for logs that Log Collectors forwarded to external services (such as a syslog server).

Issue ID	Description
PAN-83001	Fixed an issue where the firewall dropped packets based on a QoS class even though traffic did not exceed the maximum bandwidth for that class.
PAN-81924	Fixed an issue on firewalls in an HA and DHCP configuration where the Peer HA1 IP Address displayed an outdated, static IP address instead of the DHCP-assigned IP address (Device > High Availability > General).
PAN-81698	Fixed an issue where the firewall did not correctly enforce administrative account expiration settings (Device > Setup > Management > Minimum Password Complexity).
PAN-80686	Fixed an issue where the firewall reported incorrect SNMP values for the received bytes (OID iso.3.6.1.2.1.2.2.1.10) and transmitted bytes (OID iso.3.6.1.2.1.2.2.1.16) of aggregate Ethernet subinterfaces.
PAN-80569	Fixed an issue where firewalls could not connect to M-500 appliances in PAN-DB mode due to certificate validation failures. With this fix, the appliances add an IP address to the Subject Alternative Name (SAN) field when generating the certificates used for firewall connections.
PAN-80222	Fixed an issue where the firewall did not update EDL information because the firewall sent EDL queries using its default service route interface as the Source Interface instead of the EDL-specific service route you configured (Device > Setup > Services).
PAN-79989	Fixed an issue on firewalls with custom signatures configured where low memory conditions intermittently caused commit or content installation failures with the following error: Threatdatabase handler failed.
PAN-79872	Fixed an issue on PA-3000 Series and PA-5000 Series firewalls where the output of the show session info CLI command did not match the actual rate of traffic passing through the firewalls.
PAN-79319	Fixed an issue where the PAN-OS XML API returned incorrect information when you sent a call for entries in an EDL.
PAN-78903	Fixed an issue where, after you bootstrapped a VM-Series firewall, modified a template and device group on the Panorama management server, and then rebooted the firewall, Panorama displayed the firewall in the modified template and device group as well as in the original template and device group to which you assigned the firewall.
PAN-78634	Fixed an issue in Panorama templates where the Panorama management server allowed you to configure a firewall administrator Password (Device > Administrators > <administrator>) that did not meet the minimum password length settings (Device > Setup).

Issue ID	Description
	<p>> Management > Minimum Password Complexity). With this fix, Panorama prevents you from saving a firewall administrator account with a password that does not meet the minimum password length settings.</p>
PAN-76632	Fixed an issue where administrators could not log in to the firewall web interface due to the root partition running out of space because management logs continued growing without the firewall ever deleting them.
PAN-75775	Fixed an issue where SNMP managers indicated syntax errors in PAN-OS MIBs, such as forward slash (/) characters not used within quotation marks (""). You can find the updated MIBs at https://docs.paloaltonetworks.com/misc/snmp-mibs.html .
PAN-49312	Fixed an issue on PA-3000 Series firewalls where, after you manually restarted the dataplane (Device > Setup > Operations), in rare cases it spontaneously restarted repeatedly due to an FPGA calibration failure. With this fix, after detecting an FPGA calibration failure, the firewall enters maintenance mode to prompt you to power cycle the firewall for recovery.

PAN-OS 8.0.8 Addressed Issues

Issue ID	Description
PAN-92105	Fixed an issue where the Panorama Log Collectors did not receive some firewall logs and took longer than expected to receive all logs when a Collector Group had spaces in its name.
PAN-89718	Fixed an issue where PA-7000 Series firewalls rebooted continuously because the <i>brdagent</i> process stopped responding during bootup due to HSCI interface initialization.
PAN-89697	Fixed an issue on the Panorama™ virtual appliance where the NFS mount failed during system bootup.
PAN-89650	Fixed an issue where the Panorama management server did not push default Security policy rule settings (Policies > Security > Default Rules) to firewalls when the settings were inherited from a parent device group.
PAN-89646	Fixed an issue where firewalls rebooted continuously because the <i>routed</i> process stopped responding after the Panorama management server pushed invalid configurations to the firewalls. With this fix, Panorama performs an additional sanity check during push operations that causes the operations to stop with errors instead of making routed unresponsive.
PAN-89575	Fixed an issue where the firewall intermittently dropped traffic after failing to decrypt it due to proxy memory depletion.
PAN-89556	Fixed an issue where, after an administrator with the read-only superuser role changed his or her password and then an administrator with the superuser role performed a partial commit, neither administrator could authenticate to the firewall.
PAN-89349	Fixed an issue on firewalls in an active/active high availability (HA) configuration where the primary firewall, with a floating IP address bound to it, sent ARP probes containing the MAC address of the secondary firewall instead of the primary. Sending ARP probes with the incorrect MAC address caused the secondary firewall to drop traffic.
PAN-89176	Fixed an issue where firewalls in an HA configuration did not map IP addresses to the usernames of GlobalProtect™ end users because the User-ID™ manager (<i>idmgr</i>) on the active firewall continuously reset after reaching its maximum capacity for User-ID information (such as user mappings and group mappings).

Issue ID	Description
PAN-89169	Fixed an issue on VM-Series firewalls in an HA configuration where HA path monitoring failed and triggered failover.
PAN-88981	Fixed an issue where the firewall failed to generate reports based on URL Filtering logs due to a syntax error when the logs contained single quotation mark characters (').
PAN-88953	Fixed an issue where a Panorama management server in an HA configuration became unresponsive after initiating HA synchronization.
PAN-88882	Fixed an issue on the Panorama management server where the web interface displayed a 502 badgateway error and the <i>configd</i> process stopped responding after you selected the more option for a dynamic address group in a Security policy rule (Policies > Security > <rule_type> > <rule> > Source/Destination).
PAN-88809	Fixed an issue where FQDN refresh operations produced a Not Resolved error because the DNS proxy engine incorrectly stopped converting ASCII encoded characters at the second-last character instead of the last character.
PAN-88671	As an enhancement to PA-5200 Series firewalls, you can now disable or enable (default) L4 checksum checking by running the new set system setting layer4-checksum {disable enable} CLI command and then rebooting the firewall. Disabling the checking enables the firewall to allow packets it would otherwise drop when some wireless access points add a VSS-monitoring Ethernet trailer (6 bytes) to HTTP request packets.
PAN-88507	Fixed an issue where firewall performance degraded because ICMP ping packets associated with static route monitoring caused a hardware buffer leak.
PAN-88474	Fixed an issue where session offloading failed because offloaded packets related to Policy-Based Forwarding (PBF) used the incorrect PBF return MAC address.
PAN-88456	Fixed an issue where firewalls did not refresh FQDN objects during the initial boot-up phase of the bootstrapping process.
PAN-88213	Fixed an issue where firewalls that had ECMP and session offloading enabled sent offloaded traffic to the incorrect next hop.
PAN-87880	Fixed an issue where root partition utilization approached the maximum capacity because the firewall did not remove WildFire® download logs that were due for removal.

Issue ID	Description
PAN-87481	Fixed an issue where SNMP managers did not display object identifiers (OIDs) for the Ethernet1/3, Ethernet1/4, and Ethernet1/5 interfaces of M-500 appliances.
PAN-87215	Fixed an issue where a Panorama management server in an HA configuration generated group mapping synchronization errors because the passive HA peer did not verify whether the Enable reporting and filtering on groups option was disabled (Panorama > Setup > Management: Panorama Settings).
PAN-87147	As an enhancement for GlobalProtect gateways, you can now add up to 100 DNS suffixes instead of 10 for resolving the unqualified hostnames of GlobalProtect clients (Network > GlobalProtect > Gateways > <gateway> > Agent > Network Services).
PAN-87122	Fixed an issue where running the clear session all filter source CLI command eleven or more times simultaneously caused Bidirectional Forwarding Detection (BFD) flapping.
PAN-86882	Fixed an issue where the firewall dataplane slowed significantly and, in some cases, stopped responding if you used nested wildcards (*) with "." or "/" as delimiters in the URLs of a custom URL category (Objects > Custom Objects > URL Category) or in the Allow List of a URL Filtering profile (Objects > Security Profiles > URL Filtering > <URL-filtering-profile> > Overrides). With this fix, the firewall does not allow you to use nested wildcards in such cases. For details, see how Nested Wildcard in URLs May Severely Affect Performance .
PAN-86814	Fixed an issue where the Panorama management server displayed more policy rules than were applicable to the targeted Device when you selected to Preview Rules .
PAN-86676	Fixed an issue on firewalls configured as DHCP servers and deployed in an HA configuration where, after HA failover, commits failed and the following error message displayed: <code>Managementserver failed to send phase 1 to client dhcpd.</code>
PAN-86671	Fixed an issue where firewalls that had tunnel inspection enabled for GTP-U traffic did not generate END entries in Tunnel Inspection logs after the GTP-U sessions cleared.
PAN-86595	Fixed an issue on M-Series appliances in Panorama mode in an active/passive HA configuration where commit jobs were stuck at 99% and all subsequent jobs entered a pending state.


Issue ID	Description
PAN-86115	Fixed an issue where PA-7000 Series firewalls intermittently displayed incorrect usernames for Traffic logs.
PAN-86076	As an enhancement to improve security for GlobalProtect deployments, the GlobalProtect portal now includes the following HTTP security headers in responses to end user login requests: X-XSS-Protection, X-Content-Type-Options, and Content-Security-Policy.
PAN-85650	Fixed an issue on firewalls with multiple virtual systems where SSL decryption failed when you installed the Forward Trust Certificate in a specific virtual system instead of in the Shared location.
PAN-85515	Fixed an issue on PA-7000 Series and PA-5200 Series firewalls with NetFlow monitoring configured where dataplanes restarted because too many processes stopped responding.
PAN-85456	Fixed an issue where switching firewalls to FIPS-CC mode set the Base DN to None and disabled the Verify Server Certificate for SSL sessions option for LDAP server profiles that you viewed or edited in the web interface (Device > Server Profiles > LDAP).
PAN-85103	Fixed an issue where the Panorama management server stopped communicating with firewalls when the incoming log rate from firewalls exceeded the capacity of the Panorama buffers.
PAN-85066	Fixed an issue where, after the Panorama management server pushed configurations to a firewall, the firewall restarted because its <i>cordd</i> process stopped responding.
PAN-84806	Fixed an issue where firewalls in an active/active HA configuration enforced user-based policies inconsistently because port-to-username mappings did not synchronize between the primary and secondary HA peers.
PAN-84752	Fixed an issue where the firewall rebooted repeatedly because the User-ID process (<i>userid</i>) stopped responding after you committed a mobile device management (MDM) configuration that failed to connect the firewall to the MDM (Network > GlobalProtect > MDM).
PAN-84703	Fixed an issue where pushing a custom application named http or smb (Objects > Applications) from the Panorama management server to firewalls interfered with antivirus detection on the firewalls.
PAN-84445	Fixed an issue where the firewall intermittently misidentified the App-ID for SSL applications. This issue occurred when a server hosted multiple applications on the same port, and the firewall identified traffic for an application using this port on the server and then inaccurately

Issue ID	Description
	recorded other applications on this server-port combination as the previously identified application. The fix requires running the set application use-appid-cache-ssl-sni no CLI command to disable the SSL-based App-ID cache.
PAN-84406	Fixed an issue where, on a firewall configured to collect username-to-group mappings from multiple LDAP servers over SSL/TLS-secured connections (Device > Server Profiles > LDAP), the firewall rebooted because the User-ID process (<i>userid</i>) restarted several times during initialization.
PAN-84219	Fixed an issue on PA-7000 Series firewalls where the <i>logrcvr</i> process had a memory leak.
PAN-84000	Fixed an issue on the Panorama management server where, after you pushed device group settings without template settings to managed firewalls, Panorama excluded template files when you used the scp export device-state CLI command to export configurations.
PAN-83937	Fixed an issue where the VM-500 firewall stopped generating GTP logs when the session table reached 75% utilization.
PAN-83909	Fixed an issue where the WF-500 appliance sent ICMP unreachable messages from the VM Interface to the Management interface.
PAN-83495	Fixed an issue where SaaS Application Usage reports did not include logs from the Selected Zone that you specified when configuring the report (Monitoring > PDF Reports > SaaS Application Usage).
PAN-83270	Fixed an issue where firewalls generated System logs with <i>cipher decrypt-final failure</i> messages after switching from normal operational mode to FIPS-CC mode.
PAN-83153	Fixed an issue where a Panorama virtual appliance in Legacy mode that was deployed in an HA configuration did not receive logs forwarded from PA-7000 Series and PA-5200 Series firewalls.
PAN-83014	Fixed an issue on the Panorama management server where the Task Manager closed when you set the Show drop-down to All jobs after a Commit > Commit and Push operation generated errors and warnings.
PAN-82949	Fixed an issue where commits failed because the <i>routed</i> process did not delete DHCP-assigned IP addresses that you removed from firewall interfaces.
PAN-82413	Fixed an issue where the Panorama web interface displayed serial numbers instead of device names when you scheduled an update to

Issue ID	Description
	install on firewalls or Log Collectors, set the Type to Applications and Threats , and set the Recurrence to Hourly or Every 30 mins (Panorama > Device Deployment > Dynamic Updates > Schedules > <schedule>) .
PAN-82370	Fixed an issue where Android endpoints could not establish VPN tunnels to GlobalProtect gateways that you configured to Enable X-Auth Support (Network > GlobalProtect > Gateways > <gateway> > Agent > <agent> > Tunnel Settings) . With this fix, GlobalProtect gateways use SHA1 first in the order of HMAC algorithms used for authenticating endpoints that use X-Auth.
PAN-82321	Fixed an issue where the firewall rebooted because the User-ID process (<i>userid</i>) stopped responding after you performed clone or shutdown operations on VMware vCenter.
PAN-82138	Fixed an issue where, after you downgraded from PAN-OS® 8.0 to PAN-OS 7.1, firewalls without direct internet access did not display software images in the web interface (Device > Software) or CLI regardless of whether you downloaded the images from the Palo Alto Networks® Update Server (at an earlier time when the firewalls had internet access) or manually uploaded the images from another system.
PAN-82105	Fixed an issue where attempting to commit a configuration that was invalid because different interfaces had overlapping subnetworks produced a commit error message that indicated duplicate IP addresses instead of the actual error condition.
PAN-82103	Fixed an issue where VM-Series firewalls on NSX failed to install content updates retrieved from the Panorama management server.
PAN-82091	Fixed an issue where PA-220 firewalls did not provide an SNMP object identifier (OID) for system disk usage.
PAN-82048	Fixed an issue on the Panorama management server where configuring a Panorama > Scheduled Config Export based on FTP but with some fields unpopulated caused Panorama to use its default local host certificate instead of the SSL/TLS Service Profile for administrative access to the web interface (Panorama > Setup > Management).
PAN-81689	Fixed an issue where the test vpn ipsec-sa tunnel<tunnel-name>:<proxy-id-name> CLI command failed when the tunnel Name and Proxy ID values collectively exceeded 32 characters (Network > IPSec Tunnels > <tunnel> > Proxy IDs). With this fix, the firewall allows 64 characters for the combined Name and Proxy ID values.

Issue ID	Description
PAN-81637	Fixed an issue on VM-Series firewalls in Data Plane Development Kit (DPDK) mode where the <i>all_task</i> , <i>mprelay</i> , and <i>pan_dha</i> processes stopped responding.
PAN-81632	Fixed an issue where the show predefined xpath /predefined/threats CLI command did not displays threat identifiers.
PAN-81416	Fixed an issue where the Panorama management server did not display logs from PA-5000 Series or PA-7000 Series firewalls, did not display scheduled reports that included IP address fields, and did not email those reports.
PAN-81243	Fixed an issue on PA-200, PA-220, and PA-800 Series firewalls where specifying a Life Time for a master key (Device > Master Key and Diagnostics) caused the key expiration and reminder dates to have incorrect values.
PAN-81102	Fixed an issue where the tftp export stats-dump CLI command failed to generate a Stats Dump file and displayed the following error: Failed to redirect error to /var/log/pan/report_gen.log(Permission denied).
PAN-81050	Fixed an issue on M-Series appliances, PA-7000 Series firewalls, and PA-5000 Series firewalls where the <i>disk-failed</i> , <i>disk-faulty</i> , and <i>pair-disappeared</i> RAID events had only a medium severity level in System logs. With this fix, these events have a critical severity level.
PAN-80908	Fixed an issue where administrators with the device administrator role did not have the role privileges required to run the scp import software CLI command.
PAN-80889	Fixed an issue where a Panorama management server deployed behind a NAT device could not manage firewalls running PAN-OS 8.0. With this fix, you must run a new operational mode CLI command on a Panorama management server that is behind a NAT device, runs PAN-OS 8.0 or a later release, and manages firewalls running PAN-OS 8.0 or a later release. The CLI command is set dlsrvr server <FQDN> , where <FQDN> is the FQDN of the Panorama Management interface.
PAN-79367	Fixed an issue where endpoints could not authenticate to a GlobalProtect portal through client certificate authentication due to an incorrect certificate status when the portal used a Certificate Profile that specified Online Certificate Status Protocol (OCSP) to validate certificates (Network > GlobalProtect > Portals > <portal> > Authentication).

Issue ID	Description
PAN-79113	Fixed an issue where, when you used the PAN-OS XML API to request updated port-to-username mappings from a multi-user terminal server after end users logged out, and the request specified an invalid IP address for the terminal server, the response had an incomplete error message that did not indicate the invalid IP address.
PAN-78015	Fixed an issue on a Panorama management server in an HA configuration where, in rare cases, the virtual machine (VM) auth key disappeared after you rebooted the active HA peer.
PAN-77648	Fixed an issue where the show system state filter-pretty sw.dev.interface.config CLI command did not display the MAC address (hwaddr) or maximum transmission unit (mtu) for aggregate Ethernet interfaces.
PAN-77519	As an enhancement to enable comparing SNMP output with CLI output for the rate of interface connections established per second (CPS), the show counter interface CLI command displays the following new counters: TCP CPS, UDP CPS, and other CPS (for all non-TCP and non-UDP connections).
PAN-77116	Fixed an issue where the firewall displayed error messages such as the following after bootup even though bootup succeeded: Error: <code>sysd_construct_sync_importer(sysd_sync.c:328):sysd_sync_register failed: (111) Unknown error code.</code>
PAN-75340	Fixed an issue where the GlobalProtect portal did not comply with HTTP Strict Transport Security (HSTS) when redirecting users from HTTP to HTTPS upon accessing the portal login page. With this fix, HSTS is enabled to secure the redirect to HTTPS, the portal requires a valid server certificate, the endpoint browser displays a warning to users with invalid client certificates who access the login page using an IP address instead of an FQDN, and you cannot use the same FQDN for both the login page and firewall Management interface.
PAN-75068	Fixed an issue where VM-Series firewalls on NSX prevented client-server TCP sessions from closing at the correct time when you configured a reset Action in Security policy rules (Policies > Security > <rule> > Actions).
PAN-68878	Fixed an issue where firewalls in an active/active HA configuration sent packets out of order.
PAN-64376	Fixed an issue where you could not set the QoS Egress Max to more than 16,000 Mbps for an aggregate Ethernet interface (Network > QoS > <interface> > Physical Interface). With this fix, you can set the QoS Egress Max to a maximum of 60,000 Mbps.


Issue ID	Description
	 <p><i>If you downgrade from a PAN-OS 8.0 release to PAN-OS 7.1.15 or an earlier release, you must reset the QoS Egress Max to 16,000 Mbps or less to avoid commit failures.</i></p>
PAN-59996	Fixed an issue where VM-Series firewalls did not apply NAT translation to the ports in the via and contact headers of Session Initiation Protocol (SIP) sessions after you enabled Dynamic IP and Port (DIPP) NAT.
PAN-59749	Fixed an issue where the firewall intermittently dropped VPN tunnel traffic between virtual systems.

PAN-OS 8.0.7 Addressed Issues

Issue ID	Description
WF500-4510	Fixed an issue where WildFire® intermittently returned incorrect verdicts for Microsoft Office documents opened in Protected View mode.
WF500-4388	Fixed an issue where a cluster of WF-500 appliances that did not have a WildFire public cloud explicitly defined in their configurations randomly disabled public cloud communication, causing cluster commits to fail. With this fix, WF-500 appliances in a cluster always connect to wildfire.paloaltonetworks.com when you don't specify a WildFire public cloud in their configurations.
WF500-4366	Fixed an issue on a WildFire appliance cluster in a high availability (HA) configuration where the VM interface on the passive HA peer allowed inbound SSH connections.
PAN-89936	A security-related fix was made to prevent the decryption of captured sessions through the ROBOT attack (CVE-2017-17841).
PAN-89568	Fixed an issue where VM-Series and PA-5200 Series firewalls prevented the setup of GTPv2-C tunnels when <code>createsession</code> response messages had GTP cause value 18, which the firewall associated with stateful failure. With this fix, the firewalls recognize messages with that cause value as normal.
PAN-89078	Fixed an issue where PA-5220 and PA-5250 firewalls did not support the correct number of policy rules for Security, Decryption, Application Override, QoS, and Tunnel Inspection policy.
PAN-88863	Fixed an issue where PA-5200 Series firewalls intermittently dropped packets in Generic Routing Encapsulation (GRE) tunnels that used Point-to-Point Tunneling Protocol (PPTP).
PAN-88846	Fixed an issue where PA-7000 Series, PA-5200 Series, and PA-5000 Series firewalls dropped packets in VPN tunnels when processing the tunnels and traffic on separate dataplanes within the same firewall.
PAN-88775	Fixed an issue where the firewall reset memory usage every day because the <code>logrcvr</code> process had a memory leak.
PAN-88286	Fixed an issue on a Panorama management server where the web interface became inaccessible because PAN-OS did not delete

Issue ID	Description
	temporary files and therefore the root partition ran out of free storage space.
PAN-87779	Fixed an issue on VM-Series firewall on Azure where a virtual network interface card (vNIC) driver introduced a TCP packet out-of-order condition that reduced throughput.
PAN-87363	Fixed an issue where selecting to Generate Tech Support File (Device > Support) caused Bidirectional Forwarding Detection (BFD) flapping while the firewall generated the file.
PAN-87277	<p>Fixed an issue on the Panorama management server where the following PAN-OS XML API call caused the <i>configd</i> process to stop responding after you changed the Panorama configuration but did not yet commit the change:</p> <pre data-bbox="537 787 1455 905">/api/?type=op&cmd=<show><config><list><admins><partial><template></template></partial></admins></list></config></show></pre>
PAN-87160	Fixed an issue on PA-5200 Series firewalls where the dataplanes did not have enough memory to support large configurations.
PAN-87145	Fixed an issue where importing a firewall configuration into a Panorama management server deleted certain Panorama shared objects.
PAN-86903	In rare cases, fixed an issue where PA-800 Series firewalls shut themselves down due to a false overcurrent measurement.
PAN-86859	Fixed an issue where commits and other operations failed because the <i>mprelay</i> process stopped responding after you committed an interface configuration change after loading a configuration, reverting to the running configuration, or restarting the management server.
PAN-86775	Fixed an issue where firewalls in an active/active HA configuration dropped Q-in-Q traffic (traffic with nested VLAN tags) when traversing the HA3 interface.
PAN-86576	Fixed an issue where end users encountered application failures because child TCP sessions closed prematurely after their parent UDP sessions closed.
PAN-86232	Fixed an issue where the Panorama management server displayed No HIP Report Found when you clicked the log details icon (magnifying glass) for host information profile (HIP) logs.

Issue ID	Description
PAN-86226	Fixed an issue on PA-5000 Series firewalls running PAN-OS 8.0.5 or a later release where insufficient proxy memory caused decryption failures and prevented users from accessing the GlobalProtect portal or gateway.
PAN-86178	Fixed an issue where the firewall or Panorama management server did not display an error message when it ran out of free disk space, so commits failed without explanation. With this fix, the firewall or Panorama aborts commits before starting them when it has insufficient free disk space.
PAN-85744	Fixed an issue where the User-ID process (<i>userid</i>) produced an error message (Servererror : Client useridd not ready) and stopped responding during a commit operation.
PAN-85640	Fixed an issue where the firewall could not refresh external dynamic lists (EDLs) through a proxy server.
PAN-85497	Fixed an issue where, after the Panorama management server successfully downloaded a scheduled content update but firewalls or Log Collectors could not automatically retrieve and install the update at the scheduled time (because of temporary connection issues for example), Panorama did not display an Action option to Install the update manually (Panorama > Device Deployment > Dynamic Updates).
PAN-85394	Fixed an issue on the Panorama management server where you could not use the web interface to install a GlobalProtect Cloud Services plugin after modifying the plugin filename.
PAN-85348	Fixed an issue where PAN-OS indicated the master key was invalid when you configured it to use an ampersand (&) character. With this fix, the ampersand is an allowed character in the master key.
PAN-85299	Fixed an issue on firewalls in an active/passive HA configuration with link or path monitoring enabled where a failover resulting from a link or path failure intermittently caused PAN-OS to delete host, connected, static, and dynamic routes (both OSPF and BGP) from the forwarding information base (FIB) on the firewall peer that became active. The failover also caused PAN-OS to intermittently send unnecessary BGP withdrawal messages to BGP peers. With this fix, you can prevent these issues by using the new set system setting delay-interface-process interface<interface-name> delay<0-5000> CLI command (default is 0ms; range is 0 to 5000ms). This command specifies a delay period, after a link fails and before PAN-OS brings down its associated interface, to give enough time after failover for the newly active firewall HA peer to become fully active

Issue ID	Description
	and to synchronize the correct route information with its peer. In most deployments, the best practice is to set the delay to a period that is greater than the sum of the Promotion Hold Time (default 2000ms) and Monitor Fail Hold Up Time (default 0ms).
PAN-85238	A security-related fix was made to prevent a cross-site scripting (XSS) attack through the PAN-OS Captive Portal (CVE-2017-16878).
PAN-85047	Fixed an issue where the firewall failed to retrieve a domain list from an external dynamic list (EDL) server over a TLSv1.0 connection.
PAN-85035	Fixed an issue where end users could not access applications and services due to DNS resolution failures that occurred because the firewall associated the destination port with Bidirectional Forwarding Detection (BFD) packets instead of DNS packets.
PAN-84950	Fixed an issue where the Panorama management server did not push changes to the Content Update Server value of WildFire clusters after a commit on the WF-500 appliances in that cluster (Panorama > Managed WildFire Clusters > General).
PAN-84903	Fixed an issue where selecting Check Now in Device > Dynamic Updates caused PAN-OS to apply a global configuration lock that prevented any administrators from performing tasks on the firewall while it checked the Palo Alto Networks Update Server for new content updates. With this fix, PAN-OS no longer locks the configuration when checking for content updates.
PAN-84856	Fixed an issue where the firewall misidentified Signiant-based traffic as HTTP-proxy traffic and therefore did not apply policy correctly to that traffic.
PAN-84808	Fixed an issue where high packet-descriptor utilization caused the firewall to drop traffic over an IPSec tunnel that used the Authentication Header protocol for key exchange.
PAN-84781	Fixed an issue on firewalls with Decryption policy enabled where intermittent packet loss and decryption failures occurred because the firewall depleted its software packet buffer pool.
PAN-84617	<p>Fixed an issue on the Panorama management server where the Task Manager displayed Commit, Download, and Software Install tasks as stuck in a pending state after the <code>configd</code> process restarted.</p> <p> <i>This issue is not fixed for the Commit All task, which remains stuck at 0% completion after <code>configd</code> restarts.</i></p>

Issue ID	Description
PAN-84546	Fixed an issue where the Panorama management server failed to download scheduled content or Antivirus updates that overlapped with other scheduled downloads.
PAN-84186	Fixed an issue where, after the Panorama management server rebooted, it deleted known hosts for SSH sessions and therefore disrupted scheduled configuration exports (Panorama > Scheduled Config Export).
PAN-84165	Fixed an issue where, after a NetApp NFS server was temporarily unreachable, NetApp NFS clients failed to reconnect to it because the firewall blocked the challenge ACK signal required for RFC-5961 sessions. With this fix, you must run the set deviceconfig setting tcp allow-challenge-ack yes CLI command in configuration mode to enable NFS clients to reconnect with the NFS server in cases where new connections are required.
PAN-84082	Fixed an issue on the Panorama management server where the management server restarted because the <i>configd</i> process stopped responding due to memory corruption.
PAN-84018	Fixed an issue where Data Filtering logs did not display files that had spaces in their filenames.
PAN-83689	Fixed an issue on PA-5200 Series firewalls where missing LACP packets caused aggregate Ethernet groups to intermittently drop interfaces.
PAN-83678	Fixed an issue on M-Series appliances where, after you upgraded the Panorama software or added logging disks of varying sizes, the appliances stopped collecting logs from firewalls because uneven log distribution across the logging disks caused the used storage on one disk to approach the maximum capacity.
PAN-83394	Fixed an issue where a firewall on which you enabled GTP inspection allowed malformed GTP packets with invalid IMSI or MSISDN numbers to pass inspection.
PAN-82827	Fixed an issue where, after you enabled Captive Portal, the firewall stopped logging traffic for applications it identified as incomplete or undecided for <i>unknown users</i> (users that User-ID has not mapped to IP addresses).
PAN-82825	Fixed an issue where a commit failed after you increased the number of external dynamic list (EDL) objects.
PAN-82760	Fixed an issue on Panorama Log Collectors where the show log-collector-es-indices CLI command displayed errors. Also fixed

Issue ID	Description
	an issue where Collector Groups with log redundancy enabled started deleting the oldest logs when the used storage on Log Collectors approached half the maximum capacity instead of when used storage approached the full maximum capacity.
PAN-82731	Fixed an issue on the Panorama management server where System logs did not record disconnections with managed firewalls.
PAN-82497	Fixed an issue where the firewall intermittently dropped username-to-group mappings, which disrupted how it applied group-based policies.
PAN-82332	Fixed an issue where the firewall exported a configuration file of 0 bytes when you used the firewall web interface to export a configuration file (Setup > Operations).
PAN-82251	Fixed an issue where the VM-Series firewall on AWS GovCloud did not support bootstrapping.
PAN-82181	Fixed an issue where the firewall blocked access to HTTPS websites that had DigiCert-signed certificates after you configured SSL Forward Proxy decryption, configured the firewall to Block sessions with unknown certificate status (Objects > Decryption Profile > SSL Decryption > SSL Forward Proxy) , and configured certificate status validation through certificate revocation lists (CRLs).
PAN-82125	Fixed an issue where the firewall management plane or control plane continuously rebooted after an upgrade to PAN-OS 8.0, and displayed the following error message: <code>rcu_scheddetected stalls on CPUs/tasks</code> .
PAN-82117	Fixed an issue where PA-5000 Series firewalls in an active/active HA configuration intermittently dropped packets due to a race condition that occurred when the session owner and session setup were on different HA peers.
PAN-82070	Fixed an issue where PA-5020 firewalls supported a maximum bandwidth (Egress Max) of only 1Gbps for classes of service (Network > Network Profiles > QoS). With this fix, the egress max limit is 8Gbps on PA-5020 firewalls and 16Gbps on PA-5050 and PA-5060 firewalls.
PAN-81885	Fixed an issue where the firewall did not display a warning when you deleted a shared object that Security policy rules used. With this fix, the firewall displays a message indicating that policy rules use the shared object you are trying to delete and prevents you from deleting that object until you remove it from policy rules.

Issue ID	Description
PAN-81710	Fixed an issue where the Panorama management server failed to perform scheduled exports of configuration files to an FTP server (Panorama > Scheduled Config Export).
PAN-81586	A security-related fix was made to prevent a cross-site scripting (XSS) vulnerability in GlobalProtect (CVE-2017-15941).
PAN-81573	Fixed an issue where a firewall configured as a DNS proxy (Network > DNS Proxy) failed to resolve an address object with the Type set to FQDN and a name that ended with a period (Objects > Addresses).
PAN-81539	Fixed an issue where commits failed because the <i>logrcvr</i> process restarted continuously on firewalls that had NetFlow exports configured.
PAN-81171	Fixed an issue where firewalls that performed SSL decryption slowed the download of large files over HTTPS on macOS endpoints.
PAN-80645	Fixed an issue where the VM-Series firewall lost OSPF adjacency with a peer device because the firewall dropped large OSPF link state packets.
PAN-80631	Fixed an issue where the Panorama management server failed to push configuration changes filtered by administrator to managed firewalls after you configured Panorama to not Share Unused Address and Service Objects with Devices .
PAN-80542	Fixed an issue where administrators whose roles have the Privacy privilege disabled (Device > Admin Roles > Web UI) can view details about source IP addresses and usernames in scheduled reports.
PAN-80423	Fixed an issue where VM-Series firewalls in an active/passive HA configuration added a delay in traffic once every minute while sending Gratuitous Address Resolution Protocol (GARP) packets after you set the Link State to down on a Layer 3 interface (Network > Interfaces > Ethernet > <interface> > Advanced).
PAN-80395	Fixed an issue where the User-ID agent mapped IP addresses to incorrect (obscured) usernames when the firewall authenticated users through a SAML identity provider (IdP) that excluded the username attribute from SAML assertions and used a persistent name-identifier policy (<i>NameIDPolicy</i>). With this fix, the firewall no longer mandates a transient NameIDPolicy for SAML assertions; the NameIDPolicy is entirely at the discretion of the IdP.

Issue ID	Description
	 <p data-bbox="613 226 1312 321"><i>An IdP that excludes the username attribute and has a transient NameIDPolicy still sends obscured usernames to the firewall.</i></p>
PAN-80272	Fixed an issue where Data Filtering logs showed incorrect file names for file uploads and downloads.
PAN-80263	Fixed an issue where numerous simultaneous LDAP connections (in the order of tens or more) caused the connections between firewalls and User-ID agents to become stuck in the connecting state.
PAN-79753	Fixed an issue where the Panorama management server restarted after you ran the replace device old <old_SN#> new <new_SN#> CLI command to replace the serial number of an old managed firewall with that of a new managed firewall.
PAN-79671	Fixed an issue where firewalls ran out of disk space because they did not purge logs quickly enough.
PAN-79309	Fixed an issue where the firewall applied case sensitivity when matching domain names when you selected to Use domain to determine authentication profile in an authentication sequence (Device > Authentication Sequence). With the fix, the name matching is case insensitive: users can log into to a Windows domain system using a domain name with upper or lower case characters.
PAN-79302	Fixed an issue where committing configuration changes took longer than expected when you configured Security policy rules with combinations of applications and service ports.
PAN-79247	Fixed an issue where the firewall did not apply your changes in HIP objects and profiles to Security policy rules and HIP Match logs unless GlobalProtect clients reconnected to the GlobalProtect gateway.
PAN-79167	Fixed an issue on the Panorama management server where the members count became zero for all existing shared address groups after you imported a firewall configuration.
PAN-79067	Fixed an issue where the firewall treated an address object as a region object when the address object had the same name as a deleted region object.
PAN-78716	Fixed an issue on the Panorama management server and firewall where, after you added new administrator accounts and those administrators logged in, the administrative roles you assigned to those accounts had incomplete and therefore invalid configurations.

Issue ID	Description
PAN-78082	Fixed an issue where the firewall dropped sessions during SSL Inbound decryption because decryption errors caused TLS session resumption to fail.
PAN-77800	Fixed an issue where the firewall failed to generate a Simple Certificate Enrollment Protocol (SCEP) certificate when you selected a SCEP profile with the Subject containing an email address attribute (Device > Certificate Management > SCEP).
PAN-77779	Fixed an issue where the Panorama management server did not release a commit lock after a successful commit.
PAN-77673	Fixed an issue where, when testing which policy rule applied to traffic between a specified destination and source, the PAN-OS XML API query did not display as much information as the corresponding CLI command (test security-policy-match).
PAN-77526	Fixed an issue where, after you used a Panorama management server to push the Require Password Change on First Login setting to managed firewalls (Device > Setup > Management > Minimum Password Complexity), those firewalls did not prompt administrators to change their passwords during initial login.
PAN-77241	Fixed an issue on the Panorama management server and PA-7000 Series firewalls where the risk meter in the ACC tab always indicated 0 risk.
PAN-77128	Fixed an issue on the Panorama management server where the Commit > Commit and Push operation did not push the running configuration to firewalls.
PAN-77019	Fixed an issue where PA-7000 Series firewalls in an active/active HA configuration randomly dropped packets because High Speed Chassis Interconnect (HSCI) links intermittently flapped.
PAN-76404	Fixed an issue where scheduled custom reports did not correctly display column headers.
PAN-76349	Fixed an issue where a Panorama management server running PAN-OS 8.0 pushed configurations to firewalls running PAN-OS 7.1 instead of just validating the push operation after you selected to Validate Template Push (Commit > Commit and Push) .
PAN-76220	Fixed an issue where Dedicated Log Collectors failed to connect to a Panorama management server when you specified an FQDN as the Panorama Server IP (Panorama > Managed Collectors >

Issue ID	Description
	<Log_Collector> > General) due to DNS resolution failure that resulted from PAN-OS adding an extra line character to the end of the FQDN.
PAN-75741	Fixed an issue where the firewall did not generate System logs to indicate registration or connection errors that prevented it from submitting files to the WildFire cloud.
PAN-60244	Fixed an issue where the Panorama management server did not display firewall logs after you configured Panorama to access the Palo Alto Networks Update Server through a proxy server but did not specify login credentials for the proxy server (Panorama > Setup > Services).
PAN-58581	Fixed an issue where a GlobalProtect satellite sent the wrong certificate chain after you renewed the certificate authority (CA) certificates of GlobalProtect portals and gateways.

PAN-OS 8.0.6-h3 Addressed Issues

This PAN-OS® 8.0.6-h3 release includes fixes for four important issues, including the fix that enables all Palo Alto Networks® customers running a PAN-OS 8.0 release to immediately protect their networks from the post-authentication command injection vulnerability covered in CVE-2017-15940 ([PAN-81892](#); see [PAN-SA-2017-0028](#) for more details). Note that the security advisory originally misstated that this vulnerability issue (PAN-81892) was addressed in the PAN-OS 8.0.6 release. We have updated the security advisory with the correct information. We strongly recommend that you upgrade to PAN-OS 8.0.6-h3 or a later release to fix the vulnerability reported in CVE-2017-15940.

Issue ID	Description
PAN-85938	Fixed an issue where PAN-OS removed the IP address-to-username mappings of end users who logged in to a GlobalProtect™ internal gateway within a second of logging out from it.
PAN-85055	Fixed an issue where firewalls dropped TCP/UDP-based application traffic over a GlobalProtect VPN tunnel in high latency networks.
PAN-83687	Fixed an issue on Panorama™ M-Series appliances where the config process stopped responding during a Commit > Commit and Push operation in which Panorama pushed configuration changes to Collector Groups.
PAN-81892	A security-related fix was made to prevent a command injection condition through the firewall web interface (CVE-2017-15940).

PAN-OS 8.0.6 Addressed Issues

Issue ID	Description
WF500-4490	Fixed an issue where the WF-500 appliance failed to synchronize verdicts when more than 500 SHA-256 hash values required verdict checks.
WF500-4471	Fixed an issue where a WildFire® two-node high availability (HA) cluster failed to recover from a split-brain condition.
WF500-4333	Fixed an issue where WF-500 appliances running a PAN-OS® 8.0 release incorrectly allowed telnet access to the CLI on vm-interface, eth2, and eth3.
WF500-3868	<p>Fixed an issue on a WildFire appliance cluster with two controller nodes in an HA configuration where, under certain circumstances, synchronizing the controller node running configurations caused a validation error that prevented the configuration from committing on the peer controller.</p> <p>When you ran the request high-availability sync-to-remote running-configuration command on one controller node, it overwrote the candidate configuration on the peer controller and committed the new (synchronized) configuration. However, if you then changed the configuration on the peer controller and committed the change, the commit failed and returned the following error: Validation Error: template unexpected here.</p>
PAN-87749	Fixed an issue where the firewall generated too many GTP state failure logs.
PAN-86534	Fixed an issue where the log memory process (<i>logd</i>) stopped responding when Panorama received logs that were more than one week old.
PAN-86353	Fixed an issue on the Panorama management server where combinations of reports and log queries intermittently produced a slow memory leak that causes memory-related errors such as commit failures.
PAN-86061	Fixed an issue on firewalls in an active/active HA configuration where the firewall dataplane restarted after the <i>all_pktproc</i> process stopped responding due to an invalid ingress interface.
PAN-85907	Fixed an issue on Panorama appliances in Panorama or Log Collector mode where an out-of-memory condition occurred because a memory leak in the <i>reportd</i> process raised CPU usage and swap memory.

Issue ID	Description
PAN-85703	Fixed an issue where firewalls in an HA configuration intermittently dropped DHCP packets.
PAN-85674	Fixed a kernel issue that caused the firewall to reboot.
PAN-85458	Fixed an issue where the firewall listed dynamic updates with a Type set to Unknown (Device > Dynamic Updates and Panorama > Dynamic Updates).
PAN-85201	Fixed an issue on firewalls in an active/passive HA configuration where PAN-OS sent an unnecessary BGP withdrawn message to the BGP peer after the active firewall changed to a suspended HA state.
PAN-85170	Fixed an issue on firewalls that authorized virtual system administrators through RADIUS Vendor-Specific Attributes (VSAs), including the <i>PaloAlto-Admin-Access-Domain</i> VSA, where the following error message displayed after administrators accessed Monitor > Logs in the web interface: <code>syntax error at end of input</code> .
PAN-85006	Fixed an issue where PA-5200 Series firewalls did not populate the next-hop table based on your configured policy rules (Policies > Policy Based Forwarding).
PAN-84927	Fixed an issue on PA-5200 Series firewalls where the Link Speed and Link Duplex settings of copper RJ-45 ports displayed as Unknown. With this fix, the settings correctly display as auto (automatic negotiation), which is the only available option for copper ports.
PAN-84707	Fixed an issue where the firewall web service stopped responding after you configured credential phishing prevention (Objects > Security Profiles > URL Filtering > User Credential Detection).
PAN-84704	Fixed an issue where the firewall web service stopped responding after you configured credential phishing prevention (Objects > Security Profiles > URL Filtering > User Credential Detection).
PAN-84545	Fixed an issue where PA-800 Series firewalls became unresponsive until you rebooted them, and the firewalls generated no logs from when they stopped responding to when they finished rebooting.
PAN-84267	Fixed an issue where firewalls in an active/passive HA configuration stopped passing traffic when OSPF hello packets contained a duplicate router ID or when the passive peer leaked packets during a reboot.
PAN-84224	Fixed an issue where the web portal landing page for GlobalProtect Clientless VPN became unresponsive due to a race condition between

Issue ID	Description
	one user logging in to the GlobalProtect portal and another user requesting an update.
PAN-84142	Fixed an issue on a VM-Series firewall on Azure where upgrading the PAN-OS version caused a process (<i>vm_agent</i>) to stop responding due to a bug in the Azure Linux Agent library (<i>waagentlib</i>) package.
PAN-84087	Fixed an issue where users could not authenticate when you configured an authentication sequence containing an authentication profile based on RADIUS with challenge-response authentication.
PAN-84044	Fixed an issue where VM-Series firewalls in an HA configuration experienced HA path monitoring failures and (in active/passive deployments) HA failover. This fix applies only to firewalls with Data Plane Development Kit (DPDK) disabled; the bug remains unresolved when DPDK is enabled (see PAN-84045 in the Known Issues).
PAN-83826	Fixed an issue on the Panorama management server in an HA configuration where the passive HA peer did not display managed firewalls that you added to the active HA peer.
PAN-83754	Fixed an issue where a process (<i>vm_agent</i>) on a VM-Series firewall on Azure stopped responding after an update was applied on Azure.
PAN-83520	Fixed an issue where Panorama rebooted when receiving logs that contained non-UTF-8 characters.
PAN-83308	Fixed an issue on firewalls in an active/passive HA configuration where, after HA failover, the dataplane restarted on the newly active firewall while processing GlobalProtect Clientless VPN traffic.
PAN-83229	Fixed an issue on firewalls in an active/passive HA configuration where a link-monitoring failure caused a network outage after you enabled OSPF routing.
PAN-83113	Fixed an issue where the log receiver (<i>logrcvr</i>) process randomly restarted during a content update while the firewall was forwarding logs.
PAN-82957	Fixed an issue where firewalls didn't send queries for updated user mappings to User-ID agents; instead, the firewalls waited until the agents learned and forwarded new user mappings. By default with this fix, the firewall sends queries to the User-ID agents for unknown users. You can turn off the queries by running the persistent CLI command debug user-id query-unknown-ip off .

Issue ID	Description
PAN-82879	Fixed an issue on VM-Series firewalls where the dataplane restarted after you configured User-ID to collect IP address-to-username mappings from Active Directory servers.
PAN-82830	Fixed an issue where PA-5000 Series and PA-3000 Series firewalls that were running low on memory briefly became unresponsive, stopped processing traffic, and stopped generating logs.
PAN-82638	Fixed an issue where the Panorama management server did not push authentication enforcement objects to managed firewalls.
PAN-82637	Fixed an issue where the Panorama management server stopped responding after you used a PAN-OS XML API call to rename a policy rule or object and you accidentally used its old name as the new name. With this fix, Panorama stops you from renaming a rule or object with its old name and displays an error message indicating this is not allowed.
PAN-82548	Fixed an issue where the firewall incorrectly blocked URLs and generated false positives when users entered non-corporate passwords to access websites after you configured a URL Filtering profile to Use Domain Credential Filter (Objects > Security Profiles > URL Filtering > <URL_Filtering_profile> > User Credential Detection) .
PAN-82399	Fixed an issue where connection flapping between Log Collectors and firewalls running PAN-OS 8.0 prevented the firewalls from forwarding logs to the Log Collectors.
PAN-82339	Fixed an issue where PA-7000 Series, PA-5200 Series, PA-5000 Series, PA-3060, and PA-3050 firewalls dropped ARP updates after a flood of exception messages.
PAN-82329	Fixed an issue where a BFD link temporarily went down when you selected to Generate Tech Support File (Device > Support) or run the show running appinfo2ip CLI command while the <i>appinfo2ip</i> cache was full (the cache stores application-specific IP address mapping information).
PAN-82277	Fixed an issue where a firewall configured for route-monitoring sent ICMP messages with a ping ID of 0, which caused the firewall to drop the ping replies when you enabled zone protection.
PAN-82273	Fixed an issue where blocking proxy sessions to enforce Decryption policy rules caused packet buffer depletion, which eventually resulted in packet loss.

Issue ID	Description
PAN-82227	Fixed an issue where the firewall intermittently categorized most URLs as unknown and dropped SSL ClientHello packets after you upgraded the firewall to a PAN-OS 8.0 release.
PAN-82197	Fixed an issue where a Denial of Service (DoS) attack resulted in high CPU utilization on the firewall because it centralized session distribution on a single core instead of over all the cores.
PAN-82159	Fixed an issue where, after you upgraded a Panorama management server and firewalls to PAN-OS 8.0, the firewalls ignored changes to IPSec tunnel configurations that Panorama pushed, and didn't display the Panorama template icons (gear icons) for those configurations.
PAN-82151	Fixed an issue where the Panorama virtual appliance in Legacy mode intermittently stopped processing logs, which caused its firewall connections to flap.
PAN-82100	Fixed an issue where the PA-850 firewall couldn't establish an IPSec tunnel because IKE phase 2 negotiation failed on a network with latency.
PAN-82095	Fixed an issue on PA-3000 Series, PA-800 Series, PA-500, PA-220, PA-200, and VM-Series firewalls where QoS throughput dropped on interfaces configured to use a QoS profile with an Egress Max set to 0Mbps or more than 1,143Mbps (Network > Network Profiles > QoS Profile).
PAN-82085	Fixed an issue where the Panorama management server restarted in maintenance mode after you configured an incomplete Admin Role profile through the CLI and then performed a Panorama commit.
PAN-82043	Fixed an issue where the Panorama virtual appliance could not mount NFS storage because PAN-OS prepended an additional forward slash character to the configured NFS path, which made the path invalid (starting with //).
PAN-82030	Fixed an issue on PA-5200 Series and PA-3000 Series firewalls where the dataplane restarted frequently because the <i>all_pktproc</i> process stopped responding in environments with a large amount of fragmented multicast traffic.
PAN-81979	Fixed an issue where firewalls in a Layer 2 deployment with an HA configuration did not synchronize the media access control (MAC) address table between HA peers.

Issue ID	Description
PAN-81939	Fixed an issue where memory corruption caused the correlation engine process to restart.
PAN-81935	Fixed an issue on a firewall configured to perform path monitoring for a static route on a VLAN subinterface where the firewall displayed the static route as down even though the destination IP address was reachable.
PAN-81828	Fixed an issue on the Panorama management server where Commit > Commit and Push operations failed because the <i>configd</i> process was coring.
PAN-81820	Fixed an issue on PA-7000 Series and PA-5200 Series firewalls where packet captures (pcaps) didn't include packets that matched predict sessions.
PAN-81682	Fixed an issue where the firewall dataplane restarted while processing traffic after you enabled SSL Inbound Inspection but not SSL Forward Proxy decryption.
PAN-81661	Fixed an issue where PA-7000 Series and PA-5200 Series firewalls in a hairpin virtual wire deployment dropped traffic when predict sessions were created. In a hairpin deployment, traffic crosses a firewall twice, in both directions, across the same virtual wire(s) in the same zones.
PAN-81626	Fixed an issue on VM-Series firewalls where the <i>all_task</i> process stopped responding.
PAN-81585	Fixed an issue on the Panorama management server where, after you renamed an object in a device group, a commit error occurred because policies in the child device groups still referenced the object by its old name.
PAN-81583	Fixed an issue where BGP sessions between a gateway and a satellite in an LSVPN configuration started flapping after you upgraded the satellite to a PAN-OS 8.0 release.
PAN-81475	Fixed an issue where pushing configurations from a Panorama management server running PAN-OS 8.0 or 7.1 to PA-7000 Series firewalls running PAN-OS 7.1 or 7.0 caused memory leaks.
PAN-81457	Fixed an issue where the firewall stopped submitting samples to WildFire for analysis until you ran the debug wildfire reset dp-receiver CLI command.

Issue ID	Description
PAN-81321	Fixed an issue where IPSec tunnel phase 2 negotiations failed when attempting to connect to a remote peer when /32 traffic selectors were included in the configuration on the remote peer.
PAN-81312	Fixed an issue where the delete admin-sessions username CLI command did not delete sessions for the specified user.
PAN-81100	Fixed an issue on the firewall and Panorama management server where a memory leak caused several operations to fail, such as commits, FQDN refreshes, and content updates.
PAN-81022	Fixed an issue where a PA-500 firewall remained in a booting loop when you tried to access maintenance mode.
PAN-80994	A security-related fix was made to prevent remote code execution through the firewall Management (MGT) interface (CVE-2017-15944).
PAN-80892	Fixed an issue where PA-5200 Series firewalls performed slowly for traffic involving session offloading because the firewalls populated the next hop table incorrectly after receiving incorrect source MAC (SMAC) addresses in incoming packets.
PAN-80835	Fixed an issue where PA-3020 firewalls intermittently dropped sessions and displayed resources - unavailable in Traffic logs when a high volume of threat traffic depleted memory. With this fix, PA-3020 firewalls have more memory for processing threat traffic.
PAN-80831	Fixed an issue where connections that the firewall handles as an Application Level Gateway (ALG) service were disconnected when destination NAT and decryption were enabled. This fix applies only when the ALG service does not change packet lengths before and after NAT translation.
PAN-80687	Fixed an issue where the firewall dataplane restarted because the <i>all_pktproc</i> process suddenly started losing heartbeats.
PAN-80660	Fixed an issue where the firewall flooded System logs with the following message: Traffic and logging are resumed since traffic-stop-on-logdb-full feature has been disabled.
PAN-80638	Fixed an issue where the Panorama management server incorrectly displayed the job status as failed for a successful installation of a PAN-OS software update on firewalls.
PAN-80600	Fixed an issue on the PA-820 firewall where the dataplane restarted while processing HTTPS traffic after you configured a URL Filtering

Issue ID	Description
	profile to Use Domain Credential Filter (Objects > Security Profiles > URL Filtering > <URL_Filtering_profile> > User Credential Detection).
PAN-80598	Fixed an issue where, on PA-7000 Series and PA-5200 Series firewalls that had NAT policy rules with the Translation Type set to Dynamic IP (Policies > NAT > <policy_rule > > Translated Packet), sessions were stuck in an OPENING state for fragmented packets.
PAN-80571	Fixed an issue on M-Series appliances where the Panorama web interface didn't display logs in the Monitor tab after you updated the appliances to PAN-OS 8.0.3 or a later 8.0 release.
PAN-80566	Fixed an issue where PA-7000 Series and PA-5200 Series firewalls restarted after you set the source interface to an invalid option (Any, Use default, or MGT) for a NetFlow service route (Device > Setup > Services > Service Route Configuration). With this fix, the firewall displays a commit error to indicate you cannot set the source interface to an invalid option.
PAN-80511	Fixed an issue where firewalls intermittently failed to forward logs to Panorama after you configured Panorama as a log forwarding destination.
PAN-80447	Fixed an issue where, after a PAN-OS upgrade, packet buffer and descriptor utilization spiked and caused latency in network traffic.
PAN-80246	Fixed an issue where, after using a Panorama management server running PAN-OS 8.0 to Force Template Values when pushing configurations to firewalls running an earlier PAN-OS release, FQDN refreshes failed on the firewalls.
PAN-80149	Fixed an issue where the Panorama management server took longer than expected to populate source or destination address objects when you configured Security policy rules.
PAN-80099	Fixed an issue on the Panorama management server where the Deploy Content dialog listed Log Collectors, not just firewalls, when the update Type was Apps and Threats (Panorama > Device Deployment > Dynamic Updates), even though Log Collectors can receive only Apps updates.
PAN-80055	Fixed an issue where using the PAN-OS XML API to collect User-ID mappings caused slow responsiveness in the firewall web interface and CLI.

Issue ID	Description
PAN-79945	Fixed an issue where the Panorama management server could not deploy antivirus or WildFire updates to firewalls that already had later versions of the updates.
PAN-79782	Fixed an issue where the firewall web interface displayed a down status for IKE phase 1 and phase 2 of an IPSec VPN tunnel that was up and passing traffic.
PAN-79721	Fixed an issue where only administrators with the superuser dynamic role could run the show logging-status CLI command. With this fix, the command is available to administrators with dynamic or custom roles that have the permissions associated with the following role types: superuser, superreader, deviceadmin, devicereader (Device > Admin Roles > <admin_role_profile> > Command Line).
PAN-79569	Fixed an issue where a commit failed after an application name was moved to a container application.
PAN-79468	Fixed an issue on a firewall with multiple GlobalProtect portal connections where the dataplane restarted after <i>proxy_flow_alloc</i> process failures occurred.
PAN-79412	Fixed an issue where managed firewalls disconnected from an M-500 appliance after a partial commit and temporarily disappeared from the Panorama > Managed Devices list.
PAN-79378	Fixed an issue on the Panorama management server where dynamic address groups defined in child device groups didn't include matching address objects defined in the parent device groups.
PAN-79284	Fixed an issue where a firewall acting as an OSPF area border router (ABR) and configured to suppress subnetworks learned in one area from advertising in another area still advertised those subnetworks.
PAN-79182	Fixed an issue on firewalls in an active/passive HA configuration where, after you manually suspended an active HA firewall, it continued sending route withdrawn messages to BGP peers.
PAN-79063	Fixed an issue where the Panorama ACC tab and custom reports displayed data as expected for all device groups when viewed simultaneously but displayed no data when you selected and tried to view data for only a specific device group.
PAN-79044	Fixed an issue where the dataplane restarted after you enabled automatically-generated C2 signature matching (Objects > Security Profiles > Anti-Spyware).

Issue ID	Description
PAN-79037	Fixed an issue where the firewall failed to download a WF-Private content update and displayed the following error: Invalid content image, Failed to download file.
PAN-79026	Fixed an issue where the firewall Reset both client and server after you set the Antivirus profile to default in a Security policy rule even though all WildFire actions in the default profile are set to allow (Policies > Security > <security_rule> > Actions).
PAN-79000	Fixed an issue where, after using a Panorama management server running PAN-OS 8.0 to push threat exceptions from Objects > Security Profiles to firewalls running a release earlier than PAN-OS 8.0, the firewalls received invalid threat exceptions that were renamed to unknown and that retained the unique threat IDs from PAN-OS 8.0 instead of changing to the legacy threat IDs of the earlier PAN-OS release.
PAN-78936	Fixed an issue where Panorama Log Collectors didn't receive logs from firewalls because the <i>vldmgr</i> process did not come up.
PAN-78856	Fixed an issue where PA-800 Series firewalls displayed only the auto-negotiation option for the Link Speed and Link Duplex (transmission mode) of copper ports (Network > Interfaces > <interface> > Advanced). With this fix, the firewalls display all the options for copper ports: 10Mbps/half duplex, 10Mbps/full duplex, 100Mbps/half duplex, 100Mbps/full duplex.
PAN-78838	Fixed an issue where the Panorama management server generated Configuration logs that stored the passwords for VMware NSX plugins as plaintext. With this fix, Panorama encrypts the stored passwords.
PAN-78784	Fixed an issue on the Panorama management server and firewalls with multiple virtual systems where the Add button in Panorama > Monitor > Managed Custom Reports and Device > Monitor > Managed Custom Reports became unresponsive after you changed the Access Domain .
PAN-78718	Fixed an issue where a PA-7000 Series firewall running PAN-OS 8.0.6 or an earlier PAN-OS 8.0 release stopped saving and displaying new logs due to a memory leak after a Panorama management server running a PAN-OS 8.0 or later release pushed a predefined report that specified a field that is unrecognized by the firewall running the earlier PAN-OS release (Monitor > Reports > Mobile Network Reports).
PAN-78670	Fixed an issue on the Panorama management server where the output of the show logging status device <serial-number> CLI command did not display any data.

Issue ID	Description
PAN-78638	Fixed an issue where the User-ID process (<i>userid</i>) stopped responding due to initialization errors.
PAN-78617	Fixed an issue on the Panorama management server where Panorama > Managed Devices displayed the Shared Policy as Out of Sync for firewalls on which shared policy was actually in sync with Panorama.
PAN-78566	Fixed an issue where the firewall failed to export certificates that included certain special characters (\$, ', &, ", ;, and) in PKCS12 format.
PAN-78492	Fixed an issue in PAN-OS 8.0.2 to 8.0.5 releases where the firewall took longer than expected to Check Now for software or content updates (Device > Software/Dynamic Updates).
PAN-78442	Fixed an issue where PAN-OS did not generate a System log to record which administrators ran the request restart system CLI command.
PAN-78431	Fixed an issue where firewalls in an active/passive HA configuration with OSPF or BGP graceful restart enabled took longer than expected to fail over.
PAN-78397	Fixed an issue with custom URL filtering where some characters in the URL that was accessed were transformed incorrectly when the URL was displayed on the Continue and Override response page. With this fix, ampersand and other special characters are transformed using percent-encoding (for example, & = %26).
PAN-78341	Fixed an issue where the root partition ran out of space during generation of a tech support file when the output of the show user user-ids command was extremely large. With this fix, the data saved to the tech support file is modified to show only statistics instead of raw output, which prevents the output from this command from being so large that it fills up all available disk space.
PAN-78323	Fixed an issue on Panorama M-Series and virtual appliances where commits failed when virtual memory was exceeded while Panorama was attempting to copy a large number of shared nodes and simultaneously generating device group-specific configurations.
PAN-78253	Fixed an issue where incorrect IP addresses were added to the hardware block table when using a DoS Protection profile on zones with names longer than 15 characters.

Issue ID	Description
PAN-78127	A security-related fix was made to prevent the firewall Management (MGT) interface from becoming unavailable for legitimate use (CVE-2017-15942).
PAN-78100	Fixed an issue where the PAN-OS XML API query for show session distribution policy resulted in an error message (An error occurred).
PAN-78034	Fixed an issue where the Threat logs that Zone Protection profiles triggered for packet-type events did not record IMSI and IMEI values.
PAN-77974	Fixed an issue where the firewall could not establish BGP connections using a loopback interface over a large-scale VPN tunnel between a GlobalProtect satellite and gateway.
PAN-77963	Fixed an issue where a firewall that had a dynamic IP address for the Management (MGT) interface sent the IP address of the internal loopback address instead of the MGT interface as the network access server (NAS) IP address in RADIUS access requests.
PAN-77908	Fixed an issue where you could not Enable or Disable correlation objects (Monitor > Automated Correlation Engine > Correlation Objects) on a firewall for which you did not enable Multiple Virtual Systems Capability (Device > Setup > Management) .
PAN-77788	Fixed an issue where policy rules ignored changes to the risk factor in Objects > Application Filters after you upgraded the firewall to PAN-OS 8.0.
PAN-77748	Added debug enhancements to capture more details about IKE when third-party VPN clients use the X-AUTH feature.
PAN-77706	Fixed an issue on PA-7000 Series firewalls where packet capture intermittently failed.
PAN-77501	As an enhancement to the BGP fast failover feature, you can now use the set system setting fast-fail-over enable no CLI command to disable the feature (it's enabled by default) for the rare cases when it causes flapping on an unstable interface. When you disable the feature, the firewall automatically ends the BGP session with any adjacent external BGP peer immediately after the link fails (instead of waiting for the BGP hold timer to expire). With this fix, you can also re-enable the feature through the set system setting fast-fail-over enable yes CLI command.

Issue ID	Description
PAN-77384	Fixed an issue where tunnel-bound traffic was incorrectly routed through an ECMP route instead of a PBF route as expected.
PAN-77292	Fixed an issue where firewalls in an HA active/passive configuration did not always synchronize sessions.
PAN-77063	Fixed an issue where SSL Forward Proxy decryption failed for SSL/TLS websites that had unused certificate chains containing algorithms that PAN-OS did not support. With this fix, the firewall verifies only the certificate chains that the websites use.
PAN-77055	Fixed an issue where, after logging in to GlobalProtect, end users could access the Firewall PAN-OS XML API without additional authentication.
PAN-76848	Fixed an issue where a Panorama management server that is running low on memory loses some logs, processes log forwarding slowly, and loses connections to firewalls.
PAN-76505	Fixed an issue where the <i>mrelay</i> process stopped responding when processing IPv6 neighbor discovery updates.
PAN-76358	Fixed an issue on firewalls in an active/passive HA configuration where rebooting the passive HA peer caused its interfaces to flap.
PAN-76075	Fixed an issue where the User-ID process stopped responding when a virtual system that didn't have NTLM configured received NTLM requests.
PAN-75705	Fixed an issue where administrators could download a tech support file (Device > Support) even when their administrative roles did not have the corresponding privilege enabled.
PAN-75474	Fixed an issue where a firewall with a <code>disk full</code> condition could not connect to WildFire or the PAN-DB cloud after a management process restarted. The show wildfire status CLI command displayed the following message: Unable to authenticate remote CA certificate.
PAN-75438	Fixed an issue where the Panorama web interface displayed an error when you tried to create a new SSL/TLS server profile while configuring a Log Collector (Panorama > Managed Collectors > <Log_Collector> > Communication).
PAN-75264	Fixed an issue where SSL decryption failed when the destination server provided a large certificate chain such that the firewall had to process

Issue ID	Description
	a request exceeding 8,188 bytes. With this fix, the firewall has a larger buffer to accommodate requests containing large certificate chains.
PAN-75028	Fixed an issue on PA-5200 Series firewalls where you could not configure QoS on a subinterface because subinterfaces didn't display in the Source Interface drop-down (Network > QoS > <QoS_interface> > Clear Text Traffic).
PAN-74285	Fixed an issue where the Panorama management server took longer than expected to display Traffic logs for specific device groups.
PAN-74074	Fixed an issue in an HA active/passive configuration where the HA sync task did not completely remove the configuration for an ethernet1/x node on one peer firewall when ethernet1/x on the second peer firewall was empty (not configured) and that second peer firewall initiated the HA sync.
PAN-74054	Fixed an issue on firewalls in an active/passive HA configuration where a link-monitoring failure caused a delay in OSPF convergence on the firewall that became active after HA failover.
PAN-73333	Fixed an issue where the firewall did not record the sender or recipient in WildFire Submission logs for emails in which the header had no white space character between the display name and the email address.
PAN-73118	As an enhancement for generating reports that span multiple days, PAN-OS now generates such reports quicker and compresses them in storage so that you can save more reports.
PAN-70181	Fixed an issue where PA-7000 Series firewalls that ran a large number of scheduled daily reports (near 1,000 or more) eventually experienced a memory issue that caused CLI commands to fail and ultimately caused SSH connection attempts to the management IP address to fail also.
PAN-68256	Fixed an issue on PA-7000 Series firewalls in an HA configuration where the HA data link (HSCI) interfaces intermittently failed to initialize properly during bootup.
PAN-64589	Fixed an issue where administrators with custom roles could not perform packet captures or download and install software and content updates.
PAN-50641	Fixed an issue where enabling or disabling BFD for BGP, or changing a BFD profile that a BGP peer used, caused the connection to the BGP peer to flap.

PAN-OS 8.0.5 Addressed Issues

Issue ID	Description
PAN-83393	Fixed an issue where a firewall with GTP Security enabled (Device > Setup > Management > General Settings) did not mark a GTP control message packet as invalid when the packet payload had multiple access point names (APN).
PAN-82651	Fixed an issue where a memory leak caused commit failures with the following error message: <code>Threatdatabase handler failed</code> .
PAN-82616	Fixed an issue where the firewall prevented file transfers over HTTPS when the session offload feature was enabled.
PAN-82275	Fixed an issue where VM-Series firewalls dropped traffic on interfaces with QoS enabled due to QoS timeouts.
PAN-82234	Fixed an issue on M-Series appliances in Panorama mode where running scheduled reports caused a memory leak that resulted in errors such as commit failures and process termination.
PAN-82221	Fixed an issue on PA-5200 Series firewalls where the dataplane restarted because the <code>flow_ctrl</code> process stopped responding during heavy IPv6 traffic when the firewall interface that handled the traffic had 32,000 or more Neighbor Discovery Protocol (NDP) entries (Network > Interfaces > <interface_configuration> > Advanced > ND Entries).
PAN-82200	Fixed an issue where an OSPFv3 not-so-stubby area (NSSA) update for an IPv6 default route caused the <code>routed</code> process to stop responding.
PAN-82089	Fixed an issue on PA-3000, PA-5000, PA-5200, and PA-7000 Series firewalls where heavy IPv6 traffic caused session offloading to fail, which reduced throughput.
PAN-82076	Fixed an issue on PA-5200 Series and PA-7000 Series firewalls where traffic delays occurred due to packet buffer congestion after the <code>all_pktproc</code> process stopped responding because of an incorrect Policy Based Forwarding (PBF) policy rule ID that referenced an invalid egress interface.
PAN-81990	Fixed an issue on PA-5220 and PA-5250 firewalls running PAN-OS 8.0.4 where the dataplane restarted multiple times after the <code>all_pktproc</code> process stopped responding due to memory pool exhaustion.

Issue ID	Description
PAN-81951	Fixed an issue where errors associated with a Commit > Commit All Changes operation caused FQDN refresh operations to fail on the firewall. With this fix, commit failures don't cause FQDN refresh failures.
PAN-81590	Fixed an issue where a firewall intermittently dropped packets when an internal communication link failed to initialize.
PAN-81497	Fixed an issue where web pages accessed through GlobalProtect Clientless VPN did not load properly.
PAN-81287	Fixed an issue where a firewall in FIPS/CC mode intermittently switched to maintenance mode.
PAN-81218	Fixed an issue on the PA-500 firewall where OSPF was stuck in a loading state when OSPF neighbors connected over a tunnel interface.
PAN-81118	Fixed an issue where client systems could use a translated IP address-and-port pair for only one connection even if you configured the Dynamic IP and Port (DIPP) NAT Oversubscription Rate to allow multiple connections (Device > Setup > Session > Session Settings > NAT Oversubscription). This issue is fixed on all firewall models except PA-7000 Series firewalls (see PAN-99483 in Limitations and PA-5250 and PA-5260 firewalls (see PAN-99483 in Known Issues).
PAN-81031	Fixed an issue on firewalls with Captive Portal enabled where Authentication policy blocked any non-HTTP applications.
PAN-80837	Fixed an issue where, after upgrading from PAN-OS 7.1 to PAN-OS 8.0, the Panorama management server did not convert Threat logs into URL Filtering or Data Filtering logs when you had log forwarding filters based on severity levels.
PAN-80802	Fixed an issue on Panorama appliances in Panorama or Log Collector mode where an out-of-memory condition occurred because a memory leak in the <i>reportd</i> process raised CPU usage and swap memory.
PAN-80606	Fixed an issue where the firewall stopped uploading files to WildFire after you enabled Passive DNS Monitoring (Device > Setup > Telemetry) .
PAN-80535	Fixed an issue on a firewall with multiple virtual systems where policy rules defined for a specific virtual system could not access shared EDL objects.
PAN-80479	Fixed an issue where an end user could not use Kerberos single sign-on to authenticate to the GlobalProtect portal or gateway when user

Issue ID	Description
	membership in many Kerberos groups resulted in an HTTP header that exceeded the size that the firewall allowed. With this fix, the firewall allows a larger size for HTTP headers.
PAN-80465	Fixed an issue where PAN-OS never performed the Action configured in an update schedule on a firewall (Device > Dynamic Updates > <update_type_schedule>) or a Panorama management server (Panorama > Dynamic Updates > <update_type_schedule>) when the Threshold age for updates exceeded the frequency at which Palo Alto Networks released the updates. For example, if you configured the firewall with a threshold of 48 hours for Applications and Threats content updates but Palo Alto Networks released successive content updates every 24 hours, the latest update would never reach the 48-hour age threshold required to trigger the specified action. With this fix, PAN-OS checks the last five content release versions, instead of just the newest version, and performs the action for the latest version that matches the threshold you specified. For example, if content update version 701 is available for 24 hours and version 700 is available for 72 hours, and you set the threshold to 48 hours for Applications and Threats content updates, PAN-OS performs the action for version 700. PAN-OS checks the last five content release versions for Antivirus updates also.
PAN-80155	Fixed an issue where firewalls that were deployed in an active/passive high availability (HA) configuration and that acted as DHCP relay agents used physical MAC addresses instead of HA virtual MAC addresses for DHCP packets.
PAN-79977	Fixed an issue where the <i>snmpd</i> process restarted due to a memory leak that caused it to exceed the virtual memory limit.
PAN-79939	As an enhancement on VM-Series firewalls, you can now enable or disable Data Plane Development Kit (DPDK) mode during the bootstrap process. DPDK enhances firewall performance by increasing the packet processing speed of network interface cards (NICs). To enable DPDK, add the op-cmd-dpdk-pkt-io=on command to the <i>init-cfg.txt</i> bootstrap configuration file. If you disable DPDK by adding the op-cmd-dpdk-pkt-io=off command, the firewall uses Packet_mmap mode instead.
PAN-79874	Fixed an issue where end users could not send email because the <i>all_pktproc</i> process stopped responding after the firewall tried to process an empty filename in email traffic.
PAN-79844	Fixed an issue on Panorama where scheduled custom reports returned no data.

Issue ID	Description
PAN-79804	Fixed an issue where VM-Series firewalls for VMware NSX did not register on Panorama when they belonged to a device group that contained applications from a content release version that was newer than the version included with the PAN-OS software image for fresh installations.
PAN-79607	Fixed an issue where a spike in dataplane memory utilization caused bus errors and caused the dataplane and control plane to restart until you rebooted the firewall.
PAN-79575	Fixed an issue where commit operations failed and the firewall became unresponsive after responding to SNMP queries associated with certain OIDs that triggered an <i>snmpd</i> memory leak.
PAN-79555	Fixed an issue on VM-Series firewalls on Azure where dataplane interfaces did not come up as expected because they did not successfully negotiate Layer 2 settings during bootup.
PAN-79313	Fixed an issue where VM-Series firewalls did not successfully apply pre-licensed serial numbers for Cloud Security Service Provider (CSSP) licenses.
PAN-79238	Fixed an issue on firewalls in an HA configuration where HA path monitoring failed when the Ping Interval had a low value, such as 600ms (Device > High Availability > Link and Path Monitoring > <path_group_configuration>).
PAN-79174	Fixed an issue where commits took longer to complete than expected on firewalls with hundreds of policy rules that referenced application filters or application groups that specified thousands of applications.
PAN-78818	Fixed an issue where VM-Series firewalls deleted logs when you upgraded the base system disk from 40GB to 60GB.
PAN-78778	Fixed an issue where VM-Series firewalls for Hyper-V that used VLAN tagging dropped Ethernet frames that exceeded 1,496 bytes.
PAN-78770	Fixed an issue on PA-500 firewalls in an HA configuration where the HA1 interface went down due to a missed HA1 heartbeat.
PAN-78572	Fixed an issue where the Panorama management server delayed the display of new firewall logs because the <i>logd</i> process consumed too much memory.
PAN-78385	Fixed an issue where a Panorama management server running PAN-OS 8.0 did not display logs that were related to VPN tunnels or

Issue ID	Description
	authentication and that were collected from PA-7000 Series firewalls running PAN-OS 7.1 or an earlier release.
PAN-78362	Fixed an issue where the Panorama management server intermittently became unresponsive due to errors in the <i>configd</i> process.
PAN-78044	Fixed an issue where the firewall dropped packets that were destined for IP address FD00::/8 when you configured a Zone Protection profile with a Strict IP Address Check (Network > Network Profiles > Zone Protection > Packet Based Attack Protection > IP Drop) . With this fix, FD00::/8 is no longer a reserved IP address.
PAN-77939	Fixed an issue where the Panorama virtual appliance in Legacy mode purged older Traffic logs even when space was available to store new logs.
PAN-77935	Fixed an issue where, after you upgraded a firewall to PAN-OS 8.0, it forwarded the same logs to a syslog server multiple times instead of once.
PAN-77866	Fixed an issue where the authentication process (<i>authd</i>) stopped responding when a third-party device blocked the transmission of authentication packets between the firewall and an LDAP server. With this fix, authentication fails without <i>authd</i> becoming unresponsive when a third-party device blocks LDAP authentication packets.
PAN-77747	Fixed an issue where a firewall with ECMP enabled on a virtual router (Network > Virtual Routers > Router Settings > ECMP) did not load balance the traffic among egress interfaces when the traffic originated from another virtual router.
PAN-77702	Fixed an issue on Panorama in NSX deployments where dynamic address updates took several minutes to complete.
PAN-77652	Fixed an issue on PA-7000 Series firewalls where the <i>mprelay</i> process stopped responding due to a memory leak on the management plane.
PAN-77645	Fixed an issue where Dedicated Log Collectors did not forward logs to a syslog server over TCP.
PAN-77581	Fixed an issue where the web interface displayed no information in the Previous User tab (Network > GlobalProtect > Gateways > Remote Users: Info column).
PAN-77469	Fixed an issue on a Panorama management server running PAN-OS 8.0 where an administrator with a custom role who accessed the Context of

Issue ID	Description
	a managed firewall running PAN-OS 7.1 or an earlier release could not commit changes on that firewall.
PAN-77405	Fixed an issue where the PA-220 firewall incorrectly displayed packet descriptor utilization as 51% even when the firewall was not processing traffic.
PAN-77327	Fixed an issue where the PA-220 firewall did not send the correct interface indexes to NetFlow collectors, which prevented it from forwarding IP traffic statistics for analysis.
PAN-77171	Fixed an issue where the firewall discarded sessions that required the TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 cipher for SSL decryption.
PAN-76997	Fixed an issue on the PA-3020 firewall where SSL connections failed due to memory allocation issues if you configured a Decryption profile with Key Exchange Algorithms that included ECDHE (Objects > Decryption Profile > <decryption_profile> > SSL Protocol Settings) .
PAN-76830	Fixed an issue on PA-5000 Series firewalls where insufficient memory allocation caused SSL decryption errors that resulted in SSL session failures, and the firewall displayed the reason in Traffic logs as <code>decrypt-error</code> or <code>decrypt-cert-validation</code> .
PAN-76509	Fixed an issue on firewalls with multiple virtual systems where custom spyware signatures worked only on vsys1 (Objects > Custom Objects > Spyware).
PAN-76373	Fixed an issue on PA-5000 Series firewalls where using the web interface to display QoS Statistics (Network > QoS) caused the control plane and dataplane to restart due to a memory leak.
PAN-76263	Fixed an issue where the Panorama management server retained the threshold value for update schedules (Device > Dynamic Updates > <update_type_schedule>) in a template stack even after you removed the value from templates in the stack.
PAN-76155	Fixed an issue where the logs for the VM Monitoring Agent did not indicate the reason for events that cause it to exit. With this fix, the logs display debug-level details when the VM Monitoring Agent exits.
PAN-76040	Fixed an issue where configuring an aggregate interface group with interfaces of different media (such as copper and fiber optic) caused a commit failure. With this fix, an aggregate interface group can have interfaces with different media.

Issue ID	Description
PAN-76019	Fixed an issue where the dataplane restarted because the firewall used incorrect zone identifiers for deleting flows when untagged subinterfaces had parent interfaces with no zone assignment.
PAN-75890	Fixed an issue where the Applications report (Monitor > Reports > Application Reports) listed untunneled as one of the top HTTP applications even though no such application existed.
PAN-75724	<p>Fixed an issue where the PAN-OS integrated User-ID agent allowed weak ciphers for SSL/TLS connections. With this fix, the User-ID agent allows only the following ciphers for SSL/TLS connections:</p> <ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • DHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA • AES256-SHA256 • AES256-SHA • AES128-SHA256 • AES128-SHA
PAN-75371	Fixed an issue where firewalls configured to perform destination NAT misidentified applications after incorrectly adding the public IP addresses of destination servers to the App-ID cache.
PAN-74880	Fixed an issue where retrieving threat packet captures took longer than expected through the web interface (Monitor > Logs > Threat) or PAN-OS XML API.
PAN-74366	Fixed an issue on the firewall and Panorama where the management server (<i>mgmtserver</i>) process restarted after you tried to filter a policy list (Policies > <policy_type>) based on specific strings such as 00 or 000.

Issue ID	Description
PAN-74067	Fixed an issue in large-scale deployments where the User-ID process (<i>userid</i>) stopped responding due to a loop condition because firewalls configured as User-ID agents repeatedly redistributed the same IP address-to-username mappings.
PAN-73933	Fixed an issue where the log receiver (<i>logrcvr</i>) process restarted due to a memory leak after the firewall performed a log query for correlation objects or reports and the query included the Threat Category field.
PAN-73711	Fixed an issue where firewalls configured as DHCP clients did not receive IP addresses from the DHCP server because the firewalls did not set the gateway IP address (<i>giaddr</i>) value to zero in DHCP client reply messages.
PAN-72495	Fixed an issue where PA-7000 Series firewalls intermittently dropped packets from GlobalProtect end users if the GlobalProtect IKE gateway used a local interface that was in a different security zone than the physical ingress interface.
PAN-72334	Fixed an issue where firewalls did not resume forwarding logs to Log Collectors after Panorama management servers in an HA configuration recovered from a split-brain condition.
PAN-69932	Fixed an issue where the Panorama web interface and CLI responded slowly when numerous NSX plugins were in progress.
PAN-69283	As an enhancement for controlling access to GlobalProtect portals and gateways (internal or external), even when user endpoints have valid authentication override cookies, PAN-OS now matches the users against the Allow List of authentication profiles (Device > Authentication Profile > <authentication_profile> > Advanced). Modifying the Allow List is an easy way to prevent unauthorized access by users who have valid cookies but disabled accounts.
PAN-69014	Fixed an issue where the Panorama management server did not display logs collected from PA-7000 Series firewalls assigned to a child device group of the Device Group selected in the Monitor tab of the web interface.
PAN-68363	Fixed an issue where logs exported in CSV format had misaligned columns.
PAN-62675	Fixed an issue where a firewall frequently and continuously refreshed username-to-group mappings.

PAN-OS 8.0.4-h2 Addressed Issues

Issue ID	Description
PAN-78869	As an enhancement to reduce the sensitivity of your log collection infrastructure to network latency, you can now use the debug log-collector inter-log-collector data-compression set on CLI command so that Log Collectors compress the log data they send to other Log Collectors within a Collector Group. You must run the command on all the Log Collectors within a Collector Group to enable log compression. By default, log compression is disabled.
PAN-77935	Fixed an issue where, after you upgraded a firewall to PAN-OS 8.0, it forwarded the same logs to a syslog server multiple times instead of once.

PAN-OS 8.0.4 Addressed Issues

Issue ID	Description
WF500-4314	Fixed an issue where the WF-500 appliance incorrectly assigned a malicious verdict to samples due to Web Proxy Auto-Discovery Protocol (WPAD) DNS lookups.
PAN-80766	Fixed an issue where commits failed after upgrading a firewall to PAN-OS 8.0 if, before the upgrade, that firewall had a tunnel interface configured as the Source Interface for QoS cleartext traffic (Network > QoS > <QoS_interface> > Clear Text Traffic).
PAN-80445	Fixed an issue where the <i>reportd</i> process had a memory leak.
PAN-80122	A security-related fix was made to address a vulnerability that allowed XML External Entity (XXE) attacks on the GlobalProtect external interface because PAN-OS did not properly parse XML input (CVE-2017-9458).
PAN-80077	Fixed an issue on PA-7000 Series and PA-5200 Series firewalls where users failed to authenticate when the Captive Portal host session incorrectly timed out after 5 seconds.
PAN-80064	Fixed an issue where the firewall used an incorrect source MAC address for aggregate Ethernet interfaces, which caused traffic offload failures.
PAN-80062	Fixed an issue where firewalls running PAN-OS 8.0.3 displayed the error message Not authorized when administrators with local firewall accounts tried to log in using Kerberos single sign-on.
PAN-79935	Fixed an issue where the firewall dropped packets when GlobalProtect end users generated IPv6 traffic.
PAN-79833	Fixed an issue where the firewall randomly dropped packets for traffic that end users generated after connecting to GlobalProtect.
PAN-79780	Fixed an issue where the firewall could not delete old HA keys, which prevented the generation of new keys for HA1 encryption.
PAN-79779	Fixed an issue where firewall administrators that PAN-OS authenticated through RADIUS and authorized through RADIUS Vendor-Specific Attributes (VSAs) could not commit configuration changes on the firewall.

Issue ID	Description
PAN-79436	Fixed an issue where PA-7000 Series firewalls did not apply changes to the Syslog server profile configuration until you restarted the <i>syslog-ng</i> process.
PAN-79365	Fixed an issue where pushing template configurations to VM-Series firewalls for NSX removed those firewalls as managed devices on Panorama.
PAN-79311	Fixed an issue on PA-220 firewalls where, after you modified Security policy, the firewalls did not rematch the policy against sessions involving file transfers that were in progress during the policy modification.
PAN-79084	Fixed an issue where fragmented packets in GlobalProtect traffic caused PA-5200 Series firewalls to stop responding.
PAN-79001	Fixed an issue on PA-5250 and PA-5260 firewalls where QSFP ports 21 to 24 did not come up when connecting over LR optic connections.
PAN-78932	Fixed an issue where loading definitions for 8.0 SNMP MIBs failed for the PAN-TRAPS.my MIB. With this fix, you can download the latest enterprise MIBs from https://docs.paloaltonetworks.com/misc/snmp-mibs.html .
PAN-78886	Fixed an issue where the firewall ignored Authentication policy rules for websites that you added to a custom URL category.
PAN-78390	Fixed an issue where PA-5200 Series firewalls became unresponsive if they used Tap interfaces for high-throughput traffic.
PAN-78342	Fixed an issue where Panorama failed to export a custom report if you set the Database to a Remote Device Data option (Monitor > Manage Custom Reports).
PAN-78256	Fixed an issue where the firewall stopped responding and processing traffic due to a packet buffer leak.
PAN-78224	Fixed an issue where the firewall truncated passwords to 40 characters when end users tried to authenticate through RADIUS in the Captive Portal web form.
PAN-77973	Fixed an issue where the passive firewall in an active/passive HA deployment lost HA session updates when the active peer had a heavy processing load.

Issue ID	Description
PAN-77671	Fixed an issue where the firewall identified traffic to www.online-translator.com as the translator-5 application instead of as web-browsing.
PAN-77595	Fixed an issue where PA-7000 Series and PA-5200 Series firewalls forwarded a SIP INVITE based on route lookup instead of on Policy-Based Forwarding (PBF) policy.
PAN-77527	Fixed an issue where PA-5200 Series firewalls throttled packet diagnostic logs even if log throttling was disabled.
PAN-77213	Fixed an issue where Panorama failed to forward logs to a syslog server over TCP.
PAN-77096	Fixed an issue where GlobalProtect endpoints configured to use the pre-logon Connection Method with cookie authentication failed to authenticate because they failed to retrieve framed (static) IP addresses.
PAN-77062	Fixed an issue where administrators with a custom role could not delete packet captures.
PAN-77053	Fixed an issue on PA-7000 Series firewalls where the Egress Interface in a PBF policy rule (Policies > Policy Based Forwarding > <rule> > Forwarding) was reset to a null value, which brought down all the interfaces in the slot associated with the Egress Interface and caused HA failover.
PAN-77012	Fixed an issue where the firewall evaluated URL filtering-based Security policy rules without evaluating application-based rules that were higher in the rule evaluation order.
PAN-76832	Fixed an issue in virtual routers where modifying a BFD profile configuration (Network > Network Profiles > BFD Profile) or assigning a different BFD profile (Network > Virtual Routers > BGP) caused the associated routing protocol (BGP) to flap.
PAN-76831	Fixed an issue on PA-7000 Series firewalls where committing configuration changes caused the management server to stop responding and made the web interface and CLI inaccessible.
PAN-76779	Fixed an issue on the PA-5020 firewall where the dataplane restarted continuously when a user accessed applications over a GlobalProtect clientless VPN.
PAN-76381	Fixed an issue where the firewall wrote random URIs in Threat logs for Anti-Spyware DNS signatures.

Issue ID	Description
PAN-76270	Fixed an issue where operations that required heavy memory usage on Log Collectors (such as ingesting logs at a high rate) caused some other processes to restart.
PAN-76160	Fixed an issue where a large number of LDAP connections caused commit failures.
PAN-76130	A security-related fix was made to address OpenSSL vulnerabilities relating to the Network Time Protocol (NTP) library (CVE-2016-9042/ CVE-2017-6460).
PAN-76058	Fixed an issue where Panorama failed to migrate URL categories from BrightCloud to PAN-DB in policy pre-rules and post-rules.
PAN-76042	Fixed an issue where PAN-OS XML API calls for retrieving all threat details associated with a threat ID returned only threat names.
PAN-75908	Fixed an issue where multicast packets with stale session IDs caused the firewall dataplane to restart.
PAN-75769	Fixed an issue where the firewall enabled new applications associated with Applications updates received from Panorama even if you chose to Disable new apps in content update (Panorama > Device Deployment > Dynamic Updates) .
PAN-75505	Fixed an issue where the firewall failed to export a report to PDF, XML, or CSV format if the report job ID was higher than 65535.
PAN-75412	Fixed an issue where the Monitor > Botnet report displayed the wrong portion of the URL when the HTTP GET request was too long, while the Monitor > Logs > URL Filtering logs displayed the URL correctly.
PAN-75045	Fixed an issue where the firewall rejected the default route advertised by an OSPFv3 neighbor with the link-local address fe80::1.
PAN-74959	Fixed an issue where the firewall or Panorama web server stopped responding, which made the web interface inaccessible until you rebooted.
PAN-74954	Fixed an issue where firewalls did not take template settings from Panorama when you pushed a template stack that had multiple templates with a Default VSYS (Panorama > Templates > <template_configuration>) .

Issue ID	Description
PAN-74886	Fixed an issue where Panorama failed to push a shared address object to firewalls if the object was part of a dynamic address group that used a tag.
PAN-74652	Fixed an issue where, after a firewall successfully installed a content update received from Panorama, Panorama displayed a failure message for that update when the associated job ID on the firewall was higher than 65536.
PAN-74632	<p>Fixed an issue where the firewall did not clear IP address-to-username mappings or username-to-group mappings after reaching the maximum supported number of user groups, which caused commit failures with the following errors:</p> <pre data-bbox="535 730 1458 793">user-id is not registerd</pre> <p>and</p> <pre data-bbox="535 888 1458 982">ldmgr manager was reset. Commit is required to reinitialize User-ID.</pre>
PAN-74411	Fixed an issue where PAN-OS indicated only late in the bootstrapping process when the init-cfg.txt file incorrectly specified an IPv6 address without a corresponding IPv4 address, which caused the process to abort. With this fix, PAN-OS warns you of such errors much earlier in the bootstrapping process (during the sanity check phase).
PAN-74293	Fixed an issue where the firewall dropped application sessions after only 30 seconds of idle traffic instead of after the session timeout associated with the application.
PAN-74139	Fixed an issue where SSL sessions failed due to SSL decryption errors and the firewall displayed the reason in Traffic logs as decrypt - error or decrypt - cert - validation.
PAN-74110	Fixed an issue where administrators could not log in to the firewall using LDAP credentials after a PAN-OS upgrade.
PAN-73270	Fixed an issue where the firewall rebooted if a Syslog Parse profile with the Type set to Regex Identifier (Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Syslog Filters) matched a null character in a syslog message.

Issue ID	Description
PAN-73053	Fixed an issue where incremental updates failed for registered IP addresses if the firewall retrieved the updates through VM information sources (Device > VM Information Sources).
PAN-72894	Fixed an issue where Panorama failed to display HA firewalls (Panorama > Managed Devices) after the <i>configd</i> process stopped responding.
PAN-72831	Fixed an issue where rebooting the firewall caused it to generate a false critical alarm that indicated LDAP servers were down.
PAN-72698	Fixed an issue where the web interface did not display the character limit (2,048) when users tried to save log filters. With this fix, the firewall displays more information in error messages relating to saving log filters.
PAN-72342	Fixed an issue where end users ignored the Duo V2 authentication prompt until it timed out but still authenticated successfully to a GlobalProtect portal configured for two-factor authentication.
PAN-71931	Fixed an issue where Panorama allowed you to add multiple entries for the same firewall to a Log Forwarding Preferences list while configuring a Collector Group (Panorama > Collector Groups > <Collector_Group_configuration> > Device Log Forwarding), which caused a commit failure. With this fix, Panorama prevents you from adding multiple entries for the same firewall while configuring a Collector Group.
PAN-71226	Fixed an issue where the firewall dataplane restarted because packet processing processes stopped responding for HTTP traffic involving URL percent-encoding.
PAN-70119	Fixed an issue where the firewall mapped users to the Kerberos Realm defined in authentication profiles (Device > Authentication Profiles) instead of extracting the realm from Kerberos tickets.
PAN-69367	Fixed an issue where the firewall incorrectly generated packet diagnostic logs and captured packets for sessions that were not part of a packet filter (Monitor > Packet Capture).
PAN-68974	Fixed an issue on PA-3000 Series firewalls where you could not configure a QoS Profile to have a maximum egress bandwidth (Egress Max) higher than 1Gbps for an aggregate group interface (Network > Network Profiles > QoS Profile).
PAN-67618	Fixed an issue where the following Panorama XML API request to show all dynamic address groups did not respond with XML:

Issue ID	Description
	<pre>http://firewall/api/?type=op&cmd=<show><object><dynamic-address-group><all></all></dynamic-address-group></object></show></pre>
PAN-67544	Fixed an issue where, when a multicast forwarding information base (MFIB) timed out, the packet processing process (<i>flow_ctrl</i>) stopped responding, which intermittently caused the firewall dataplane to restart.
PAN-63905	Fixed an issue where RTP sessions that were created from predict sessions went from an active state to a discard state after you installed a content update or committed configuration changes on the firewall.
PAN-61834	Fixed an issue where the firewall captured packets of IP addresses not included in the packet filter (Monitor > Packet Capture).
PAN-57490	Fixed an issue where Panorama displayed an error message if you configured an access domain with 512 or more device groups. With this fix, you can configure up to 1,024 device groups in a single access domain.
PAN-54531	Fixed an issue where the firewall stopped writing new Traffic and Threat logs to storage because the Automated Correlation Engine used disk space in a way that prevented the firewall from purging older logs.

PAN-OS 8.0.3-h4 Addressed Issues

Issue ID	Description
PAN-79424	Fixed an issue where the firewall dropped packets when GlobalProtect end users generated traffic with large packets.
PAN-79051	Fixed an issue where the firewall could not process packets that had base64 chaffing applied.
PAN-78934	Fixed an issue where the firewall did not apply policy rules to HTTP traffic that matched security profile signatures when the traffic was chunked and had a small chunk size.

PAN-OS 8.0.3 Addressed Issues

Issue ID	Description
WF500-4291	Fixed an issue where the WF-500 appliance returned false positives for known, benign Portable Executable (PE) files.
PAN-78448	Fixed an issue where the firewall dropped some logs that it was configured to forward to syslog servers.
PAN-77849	Fixed an issue where the Captive Portal web form did not display to end users after you pushed device group configurations from a Panorama management server running Panorama 8.0 to a firewall running PAN-OS 7.1.
PAN-77802	Fixed an issue where every commit cleared tunnel flow sessions such as GRE and IPsec ESP/AH sessions.
PAN-77520	Fixed an issue on PA-7000 Series firewalls with AMC hard drives, model ST1000NX0423, where the firewalls rebuilt Disk Pair B in the LPC card after a reboot.
PAN-77516	A security-related fix was made to address a Remote Code Execution (RCE) vulnerability when the PAN-OS DNS Proxy service resolved FQDNs (CVE-2017-8390).
PAN-77400	Fixed an issue on a firewall running PAN-OS 8.0.1 or 8.0.2 where you could not log in to the web interface after performing a private data reset.
PAN-77339	Fixed an issue where the SafeNet Client 6.2.2 did not support the necessary MAC algorithm (HMAC-SHA1) to work with Palo Alto Networks firewalls that ran in FIPS-CC mode.
PAN-77290	Fixed an issue where Panorama displayed a missing vsys error message when you tried to update dynamic address groups through PAN-OS XML API calls, even if you specified a virtual system.
PAN-77250	Fixed an issue where the firewall lost offloaded sessions on a subinterface that belonged to an aggregate interface group and that had QoS enabled.
PAN-77173	A security-related fix was made to prevent remote code execution within the Linux kernel that the firewall management plane uses (CVE-2016-10229).

Issue ID	Description
PAN-77127	Fixed an issue where the firewall reduced the range of local and remote IKEv2 traffic selectors in a way that disrupted traffic in a VPN tunnel that a Cisco Adaptive Security Appliance (ASA) initiated.
PAN-77033	Fixed an issue where using a Panorama management server running PAN-OS 8.0 to generate a report that queried an unsupported log field from a PA-7050 firewall running PAN-OS 7.1 slowed the performance of Panorama because the <i>mgmtsvr</i> process stopped responding.
PAN-76964	Fixed an issue where interfaces went down due to packet buffers being overwhelmed after the firewall tried to close the connection to a rogue client that ignored the URL Filtering block page.
PAN-76890	Fixed an issue where traffic that included a ZIP file caused the <i>all_task</i> process to restart and the firewall dropped packets while waiting for that process to resume.
PAN-76746	Fixed an issue on the PA-7080 firewall where authentication traffic from a wireless controller to a RADIUS server failed due to buffer depletion on the firewall.
PAN-76651	Fixed an issue where VM-Series firewalls dropped multicast traffic if you enabled Data Plane Development Kit (DPDK) on VMXNET3 interfaces.
PAN-76650	Fixed an issue where renaming a shared object on Panorama that Panorama has pushed to firewalls caused a commit failure if the firewalls referenced that object in local policies.
PAN-76615	Fixed an issue where Panorama failed to Generate Tech Support File (Panorama > Support) .
PAN-76565	Fixed an issue where dynamic content updates failed on the firewall when DNS response times were slow.
PAN-76454	Fixed an issue on PA-7000 Series and PA-5200 Series firewalls where Generic Routing Encapsulation (GRE) session creation failed when the firewalls received GRE packets with a Point-to-Point Protocol (PPP) payload.
PAN-76330	Fixed an issue where the <i>pan_task</i> process stopped, which caused a loss of service and interruption to OSPF.
PAN-76271	Fixed an issue where you could not access the Panorama web interface or CLI because the <i>configd</i> process stopped after a Preview Changes operation (Commit > Commit to Panorama).

Issue ID	Description
PAN-76184	Fixed an issue on PA-7000 Series and PA-5200 Series firewalls where disabling the option to Turn on QoS feature on this interface (Network > QoS) reduced throughput on 40Gbps interfaces.
PAN-76162	Fixed an issue where Panorama 8.0 did not display logs from PA-7000 Series firewalls running PAN-OS 7.0 or PAN-OS 7.1.
PAN-76158	Fixed an issue where the firewall, when processing heavy traffic, did not properly identify and block the Psiphon application when the Psiphon client was configured to use a specific source country.
PAN-76153	Fixed an issue where PA-5000 Series firewalls dropped traffic because predict sessions incorrectly matched Policy-Based Forwarding (PBF) policy rules for non-related sessions.
PAN-76144	Fixed an issue where throughput was reduced on PA-5000 Series firewalls that used a single UDP session on one dataplane to process high rates of tunneled traffic. With this fix, you can use the set session filter-ip-proc-cpu CLI command to use multiple dataplanes to process traffic for up to 32 destination server IP addresses. This setting persists after reboots and upgrades.
PAN-76032	Fixed an issue where the firewall web interface displayed a misspelling in the tooltip that opened when you hovered over Commit when no configuration changes were pending.
PAN-76003	A security-related fix was made to prevent cross-site scripting (XSS) attacks through the GlobalProtect external interface (CVE-2017-12416).
PAN-75977	Fixed an issue where users failed to authenticate through a Ucopia LDAP server.
PAN-75617	Fixed an issue where the firewall performed the default signature action for threat vulnerability exceptions instead of performing the Action you set in the Vulnerability Protection profile (Objects > Security Profiles > Vulnerability Protection > Exceptions).
PAN-75580	Fixed an issue where a PAN-OS XML API query to fetch all dynamic address groups failed with an <code>Opening and ending tag mismatch</code> error due to command buffer limitation.
PAN-75512	Fixed an issue where the firewall failed to decrypt VPN traffic for packets of certain sizes if you set the Encryption algorithm to aes-256-gcm in the IPSec Crypto profile used for the VPN tunnel (Network > Network Profiles > IPSec Crypto).

Issue ID	Description
PAN-75413	Fixed an issue where DHCP servers did not assign IP addresses to new end users (DHCP clients) because the firewall failed to process and relay DHCP messages between the servers and clients after you configured a firewall interface as a DHCP relay agent.
PAN-75372	Fixed an issue where Panorama dropped all administrative users because the <i>management-server</i> process restarted.
PAN-75337	Fixed an issue where CPU usage spiked on the firewall during Diffie-Hellman (DHE) or elliptical curve Diffie-Hellman (ECDHE) key exchange for SSL decryption. With this fix, the firewall has enhanced performance for DHE and ECDHE key exchange.
PAN-75304	Fixed an issue where the firewall populated default values for IPSec Crypto profiles that did not have an IPSec Protocol (ESP or AH) defined (Network > Network Profiles > IPSec Crypto); the default values caused an IKE configuration parsing error that prevented IPSec VPN tunnels from coming up.
PAN-75215	Fixed an issue where the active firewall in an HA deployment kept sessions active for an hour instead of discarding them after 90 seconds when the sessions matched the URL category in a policy rule that was set to deny.
PAN-75158	Fixed an issue with network outages on firewalls in a virtual wire HA configuration with HA Preemptive failback enabled (Device > High Availability > General > Election Settings) due to Layer 2 looping after failover events while the firewalls processed broadcast traffic.
PAN-75154	Fixed an issue where the Monitor > Traffic Map displayed the Northwestern Somali region as Solomon Islands instead of Somalia.
PAN-75119	Fixed an issue where IP Address Exemptions in Anti-Spyware profiles (Objects > Security Profiles > Anti-Spyware Profile) did not work for certain threats.
PAN-75118	Fixed an issue where commits failed after you added an IPv6 peer group to a virtual router that had Border Gateway Protocol (BGP) enabled (Network > Virtual Routers > BGP > Peer Group) and that had import, export and aggregate rules configured.
PAN-75029	Fixed an issue where the PA-5060 firewall randomly dropped packets and displayed the reason in Traffic logs as <code>resources unavailable</code> .

Issue ID	Description
PAN-74938	Fixed an issue on PA-3000 Series firewalls where SSL sessions failed due to memory depletion in the proxy memory pool; Traffic logs displayed the reason decrypt - error.
PAN-74865	Fixed an issue where Panorama could not push address objects to managed firewalls if zones specified the objects in the User Identification ACL include or exclude lists (Network > Zones) and if you configured Panorama not to Share Unused Address and Service Objects with Devices (Panorama > Setup > Management > Panorama Settings).
PAN-74639	Fixed an issue where the root partition on the firewall was low on disk space (requiring you to run the debug dataplane packet-diag clear log log CLI command to free disk space) because the <i>pan_task</i> process generated logs for H.225 sessions.
PAN-74601	Fixed an issue on Panorama where Device Group and Template administrators who had access domains assigned to their accounts could not edit shared security profiles (Objects > Security Profiles) after committing those profiles.
PAN-74579	Fixed an issue where the debug dataplane internal pdt oct show-all CLI command restarted the firewall dataplane.
PAN-74440	Fixed an issue where the firewall generated System logs indicating the <i>l3svc</i> process stopped repeatedly because the <i>cryptod</i> daemon deleted a certificate key associated with an SSL/TLS Service Profile that was used for the URL Admin Override feature (Device > Setup > Content ID) or for Captive Portal (Device > User Identification > Captive Portal Settings).
PAN-74369	Fixed an issue where modifying the BFD profile in a virtual router (Network > Virtual Routers) caused the <i>routed</i> process to stop.
PAN-74334	Fixed an issue on Panorama where the replace device CLI command did not replace the serial numbers of firewalls that policy rules referenced as targets.
PAN-74243	Fixed an issue where, after you used a Panorama template to push DNS server IP addresses (Device > Setup > Services) to a bootstrapped VM-Series firewall, the firewall failed to resolve FQDNs.
PAN-73919	Fixed an issue where you could not use the web interface or CLI to configure a multicast IP address as the Source or Destination in packet filters (Monitor > Packet Capture).
PAN-73916	Fixed an issue where, after you logged in to the firewall with an administrator account that does not have a superuser role and you then

Issue ID	Description
	tried to Disable an application (Objects > Applications > <application-name>), the firewall displayed an error message that did not indicate the need for superuser privileges.
PAN-73707	Fixed an issue where you could not generate a SCEP certificate if the SCEP Challenge (password) had a semicolon (Device > Certificate Management > SCEP).
PAN-73631	Fixed an issue where end user clients failed on their first attempt to authenticate when you configured Captive Portal for certificate-based authentication and the client certificates exceeded 2,000 bytes.
PAN-73556	Fixed an issue where the firewall did not delete multicast forwarding information base (FIB) entries for multicast groups that stopped receiving traffic.
PAN-73551	Fixed an issue where commits failed with the error <code>syntax error [kmp_sa_lifetime_time ;]</code> if the firewall had IKE Crypto profiles without a Key Lifetime defined (Network > Network Profiles > IKE Crypto).
PAN-73548	Fixed an issue where the firewall used the global service route (Device > Setup > Services > Global) instead of service routes defined for specific virtual systems (Device > Setup > Services > Virtual Systems) if you configured Device > Server Profiles in the Shared location.
PAN-73484	Fixed an issue where the firewall server process (<i>devsvr</i>) restarted during URL updates.
PAN-73281	Fixed an issue where the firewall dropped multicast traffic on an egress VLAN interface when the traffic was offloaded.
PAN-73254	Fixed an issue where, after you installed the VMware NSX plugin on Panorama in a high availability (HA) configuration, Panorama did not automatically synchronize configuration changes between the HA peers unless you first updated settings related to the NSX plugin.
PAN-73184	Fixed an issue where successive HTTP GET requests in a single session failed if you configured SSL Decryption with the Strip X-Forwarded-For option enabled (Device > Setup > Content-ID).
PAN-72946	Fixed an issue where HA firewalls displayed as <code>out of sync</code> if an SSL/TLS Service Profile without a certificate was assigned to the management (MGT) interface (Device > Setup > Management). With this fix, PAN-OS unassigns the SSL/TLS Service Profile if it doesn't have a certificate.

Issue ID	Description
PAN-72863	Fixed an issue where the PAN-OS integrated User-ID agent or Windows-based User-ID agent stopped responding because the firewall sent numerous queries
PAN-72753	Fixed an issue where you could not configure the 0.0.0.0/1 subnet as a Proxy ID for IPSec VPN tunnels.
PAN-72433	Fixed an issue where the PA-7050 firewall displayed incorrect information for the packet counts and number of bytes associated with traffic on subinterfaces. With this fix, the firewall displays the correct information in the show interface CLI command output and in other sources of information for subinterfaces (such as SNMP statistics and NetFlow record exports).
PAN-72258	Fixed an issue where pushing an ARP load-sharing configuration (Device > High Availability > Active/Active Config > Virtual Address) from Panorama to a firewall deleted it from the firewall.
PAN-71922	Fixed an issue where the firewall did not generate Threat logs for classified DOS protection profiles that had an Action set to SYN Cookies (Objects > Security Profiles > DoS Protection > Flood Protection > SYN Flood) .
PAN-71535	Fixed an issue on Panorama where Panorama > Device Deployment > Software stopped displaying software images for a release after you performed a manual Upload for a software image of that release.
PAN-71133	Fixed an issue on where the dataplane rebooted after multiple dataplane processes restarted due to memory corruption.
PAN-69449	Fixed an issue where, after a clock change on the firewall (such as for Daylight Savings Time), the ACC did not display information for time periods before the change.
PAN-68808	Fixed an issue on the PA-7050 firewall where the <i>mprelay</i> process experienced a memory leak and stopped responding, which caused slot failures and HA failover.
PAN-68580	Fixed an issue where HA VM-Series firewalls displayed the wrong link state after a link-monitoring failure.
PAN-66076	Fixed an issue where the GlobalProtect portal prompted end users to enter a one-time password (OTP) even after the users entered the OTP for the GlobalProtect gateway and Authentication Override is enabled (Network > GlobalProtect > Portals > <portal-configuration> > Agent > <agent-configuration> > Authentication).

Issue ID	Description
PAN-64639	Fixed an issue where HA firewalls failed to synchronize the PAN-DB URL database.
PAN-62159	Fixed an issue where the firewall did not generate WildFire Submission logs when the number of cached logs exceeded storage resources on the firewall.
PAN-59372	Fixed an issue where neither Panorama nor the firewall generated a System log indicating a password change after you used a Panorama template to push an administrator password change to the firewall.
PAN-56287	Fixed an issue where the firewall discarded VoIP sessions that had multicast destinations.
PAN-46374	Fixed an issue on PA-7000 Series firewalls where you had to power cycle the Switch Management Card (SMC) when it failed to come up after a soft reboot (such as after upgrading the PAN-OS software).

PAN-OS 8.0.2 Addressed Issues

Issue ID	Description
WF500-4218	Fixed an issue where, as part of and after upgrading a WildFire appliance to a PAN-OS 8.0 release, using the request cluster reboot-local-node CLI command to reboot a cluster node intermittently caused the node to go offline or fail to reboot.
WF500-4186	Fixed an issue in a three-node WildFire appliance cluster where, if you decommissioned the backup controller node or the worker node (request cluster decommission start) and then deleted the cluster-related configuration (high-availability and cluster membership) from the decommissioned node, the cluster intermittently stopped functioning. Running the show cluster membership CLI command on the primary controller node showed the message: Service Summary: Cluster:offline, HA:peer-offline. In this state, the cluster did not function and did not accept new samples for processing.
WF500-4176	Fixed an issue where, after you removed a node from a cluster that stored sample information on the node, the node serial number appeared in the list of storage nodes when you displayed the sample status (show wildfire global sample-status sha256 equal <value>) even though the node no longer belonged to the cluster.
WF500-4173	Fixed an issue where integrated reports were not available for firewalls connected to a WF-500 appliance running in FIPS mode.
WF500-4158	Fixed an issue where selecting Reboot device after Install when upgrading WildFire appliance clusters from Panorama caused an ungraceful reboot that intermittently made the cluster unresponsive.
PAN-81061	Fixed an issue where PA-3000 Series firewalls dropped long-lived sessions that were active during a content update followed immediately by an Antivirus or WildFire update.
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.

Issue ID	Description
PAN-76424	Fixed an issue where Security Lifecycle Review reports (Generate Stats Dump File under Device > Support) 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 Could not connect to Cloud : SSL/TLS Authentication Failed even though the firewall had no connection failures.
PAN-76331	Fixed an issue where, after upgrading to PAN-OS 8.0.1, a Network > DNS Proxy object with ten or more Static Entries 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 Host field to an FQDN instead of an IP address.
PAN-76092	Fixed an issue where reports delivered through the Email Scheduler (Monitor > PDF Reports > Email Scheduler) 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.

Issue ID	Description
PAN-76054	Fixed an issue where you could not delete a tunnel interface from a Panorama template (Network > Interfaces > Tunnel).
PAN-76051	Fixed an issue where you could not push a Management (MGT) interface configuration from a Panorama template (Device > Setup > Interfaces) to firewalls unless you specified an IP Address 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 (Network > Virtual Routers > Routing > Static Route Monitoring) or CLI (show routing path-monitor).
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 a regression introduced in PAN-OS 8.0.0 and 8.0.1 caused the firewall dataplane to restart in certain cases when combined with content updates. For details, including the relevance of content release version 709, refer to the associated Customer Advisory .
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 Type to None (Device > Authentication Profile) 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 <i>configd</i> 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

Issue ID	Description
	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-74934	Fixed an issue where, after upgrading M-500 private cloud appliances to a release later than PAN-OS 8.0.0, queried URLs did not resolve to a category when they were a best match to an entry in the URL database that had many subdomains and path levels. With this fix, you can upgrade the appliances to PAN-OS 8.0.2; do not upgrade the appliances to PAN-OS 8.0.1.
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 where users experienced slow network connectivity due to CPU utilization spikes in the firewall 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.
PAN-74613	Fixed an issue where the show running url-cache statistics 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 Type from DHCP Client to Static .
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 Action set to No Decrypt , you could not use the web interface to set the decryption Type for matching traffic.

Issue ID	Description
PAN-74403	Fixed an issue on Panorama where the web interface became unresponsive after you selected Export to CSV for a custom report, which forced you 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 a policy rule references does not impact 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 Enforce Symmetric Return .
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 when the DHCP leases expired.
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 following error: Invalid user name.
PAN-73710	Fixed an issue where the firewall did not commit changes to the NTP servers configuration (Device > Setup > Services) if the firewall

Issue ID	Description
	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 (Device > High Availability > General) 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 end 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 Portal Login Page was set to Disable (Network > GlobalProtect > Portals > General) and the user entered https://portal in the browser URL field, the browser redirected to https://portal/global-protect/login.esp , 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 a heavy processing load on the dataplane and queued OSPF hello packets.
PAN-73045	Fixed an issue where HA failover and fail-back events terminated sessions that started before the failover.
PAN-72871	Fixed an issue where the firewall displayed only part of the URL Filtering Continue and Override 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.

Issue ID	Description
PAN-72149	Fixed an issue where URL values did not display for the top websites in URL Filtering reports (Monitor > PDF Reports > Manage PDF Summary).
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 use the request hsm client-version CLI command to select the version that is compatible with your SafeNet HSM server.
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).
PAN-70731	Fixed an issue where the firewall failed to authenticate to a SafeNet hardware security module (HSM) if the Administrator Password (under Device > Setup > HSM) contained special characters.
PAN-70353	Fixed an issue where GlobalProtect Clientless VPN did not work when its host was a GlobalProtect portal that you configured on an interface with DHCP Client enabled (Network > Interfaces > <interface> > IPv4).
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 Enable User Identification Timeout option disabled, the firewall assigned the mappings a timeout of 60 minutes instead of never (Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Cache).
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 Generate

Issue ID	Description
	Tech Support File under Device > Support) includes additional registry values to troubleshoot path monitoring failures.
PAN-67412	Fixed an issue on firewalls in an HA configuration where, when an end user accessed applications over a GlobalProtect clientless VPN, the web browser became unresponsive for about 30 seconds after a 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 end 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 Monitor > App Scope > Network Monitor displayed incorrect byte totals and hourly distribution when you filtered the report by Source User/Address or Destination User/Address instead of by Application .
PAN-63205	Fixed an issue on VM-Series firewalls where commit operations failed after you configured HA with the HA2 and HA3 interfaces.
PAN-62791	Fixed an issue where the firewall could not use the certificates in its certificate store (Device > Certificate Management > Certificates > Device Certificates) after a manual or automatic commit, which caused certificate authentication to fail.
PAN-62074	Fixed an issue where the User-ID agent incorrectly read the IP address in the security logs for Kerberos login events.
PAN-61644	Fixed an issue where Panorama displayed the Invalid term(device-group eq) error when you tried to display the logs for a specific device group.
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 Tag Allowed value for virtual wire interfaces (Network > Virtual Wires), which caused a commit error because the

Issue ID	Description
	option is not configurable on that firewall model. With this fix, the Tag Allowed value has a read-only value of 0-4094 on VM-Series firewalls for NSX.
PAN-56015	Fixed an issue where the syslog format for Correlation logs differed from the format of other log types, which prevented the firewall from integrating with some third-party syslog feeds.
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.
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

Issue ID	Description
WF500-4098	Fixed an issue in a WildFire appliance cluster that had three nodes where decommissioning the active (primary) controller node failed.
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 $<n>$, where $<n>$ is the UTC+ $<n>$ value for the current time zone.
PAN-73964	Fixed an issue where you could not upgrade VM-Series firewalls on AWS in an HA configuration 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 Metadata 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

Issue ID	Description
	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.
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-73168	Fixed an issue where your web browser displayed the error message 400 Bad Request when you tried to access a PAN-OS web interface that shared the same FQDN as the GlobalProtect portal that hosted Clientless VPN applications.
PAN-73006	Fixed an issue where the App Scope Change Monitor and Network Monitor reports failed to display data if you filtered by Source or Destination 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-72875	Fixed an issue where the severity level of the Failed to sync PAN-DB to peer: Peer user failure syslog message was too high. With this fix, the message severity level is info instead of medium.
PAN-72849	Fixed an issue in Panorama HA active/passive configurations where Elasticsearch parameters were not pushed to the passive peer.

Issue ID	Description
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 Panorama web interface and CLI displayed a negative value for the Log Storage capacity (Panorama > Collector Groups > <Collector_Groups > General).
PAN-72547	Fixed an issue where running the clear session all 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, after you configured a BGP IPv6 aggregate address with an Advertise Filter that had both a prefix filter and a next-hop filter, the firewall advertised only the aggregate address and did not advertise the specific routes that the Advertise Filter covered (Network > Virtual Routers > <router> > BGP > Aggregate > <address> > Advertise Filters > <advertise_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-71833	Fixed an issue where the output of the test authentication authentication-profile CLI command intermittently displayed authentication/authorizationfailed for user for TACACS+ authentication profiles even though the administrator could successfully log in to the web interface or CLI using the same credentials as were specified in the test command.
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).

Issue ID	Description
PAN-71312	Fixed an issue where custom reports did not display results for queries that specified the Negate option, Contains operator, and a Value 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.
PAN-70436	A security-related fix was made to prevent tampering with files that are exported from the firewall web interface (CVE-2017-7217/PAN-SA-2017-0008).
PAN-70366	Fixed an issue where SMTP email servers did not receive PDF reports from the firewall because the report emails had line separators that used bare LF instead of CRLF.
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: <pre data-bbox="537 947 1456 1037">Import of <cert name> failed. Unsupported digest or keys used in FIPS-CC mode.</pre>
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-69340	Fixed an issue where PAN-OS did not apply the capacity license when you used a license authorization code (capacity license or a bundle) to bootstrap a VM-Series firewall because the firewall did not reboot after the license was applied.
PAN-68795	Fixed an issue where the SaaS Application Usage report displayed upload and download bandwidth usage numbers incorrectly in the Data Transfer by Application section.
PAN-68185	Fixed an issue where the 7.1 SNMP traps MIB (PAN-TRAPS.my) had an incorrect description for the <i>panHostname</i> attribute.
PAN-67952	Fixed an issue on PA-5000 Series firewalls where the dataplanes became unstable when jumbo frames and first packet broadcasting

Issue ID	Description
	were both enabled. With this fix, first packet broadcasting is disabled by default on PA-5000 Series firewalls.
PAN-67629	<p>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:</p> <pre data-bbox="537 506 1456 659">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	Firewalls did not support tunnel content inspection in a virtual-system-to-virtual-system topology.
PAN-64725	Fixed an issue where Panorama did not maintains its connections to firewalls if it received logs at a high rate and the logs matched queries and other settings in scheduled reports.
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-62820	Fixed an issue for the Apple Safari browser in Private Browsing mode where the firewall did not redirect you to the service or application—even when authentication succeeded—when you requested a service or application that required multi-factor authentication (MFA).
PAN-61840	Fixed an issue where the show global-protect-portal statistics CLI command was not supported.
PAN-60101	Fixed an issue on the M-500 and M-100 appliances in Panorama mode where emailed custom reports contained no data if you configured a report query that used an Operator set to contains (Monitor > Manage Custom Reports) .
PAN-59677	A security-related fix was made to prevent firewall administrators logged in as root from using GNU Wget to access remote servers and

Issue ID	Description
	write to arbitrary files by redirecting a request from HTTP to a crafted FTP resource (CVE 2016-4971).
PAN-58979	Fixed an issue where the dataplane restarted due to a memory leak (<i>mprelay</i>) that occurred if you did not disable LLDP when you disabled an interface with LLDP enabled (Network > Interfaces > <interface> > Advanced > LLDP).
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

Issue ID	Description
PAN-76702	Fixed an issue where several dataplane processes stopped responding on the firewall after it applied SSL Forward Proxy Decryption policy to traffic that then traversed a VPN tunnel.
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 (<i>dnsproxy</i>) stopped running on a firewall that had an address object (Objects > Address) with the same FQDN as one of the Static Entries in a DNS proxy configuration (Network > DNS Proxy).
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 BPDUs through an interface that had previously physically flapped.
PAN-71311	Fixed an issue where, if you configured a User-ID agent with an FQDN instead of an IP address (Device > User Identification > User-ID Agents), the firewall generated a System log with the wrong severity level (informational instead of high) after losing the connection to the User-ID agent.
PAN-71307	Fixed an issue where the scp export stats-dump report did not run correctly because source (src) and destination (dst) 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

Issue ID	Description
	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 (Network > Virtual Wires), 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).
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-69901	Fixed an issue where the hyphen ("-") character was not supported in a DNS proxy domain name (Network > DNS Proxy > <dns-proxy-name> > DNS Proxy Rules > <rule-name> > Domain Name).
PAN-69235	Fixed an issue where committing a configuration with several thousand Layer 3 subinterfaces caused the dataplane to stop responding.
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 Drop . With this fix, Panorama translates the action from Drop to Drop packets 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 (Network > GlobalProtect > Gateways) became inactive and prevented you from reopening the User Information dialog if you closed the dialog using the Esc key instead of clicking Close .

Issue ID	Description
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 Number of Hits (SSH hello messages) to 3 and per seconds to 60 , 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 (Monitor > Logs > Unified) 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 did not populate User-ID mappings based on the defined Syslog Parse profiles (Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Syslog Filters).
PAN-68074	A security-related fix was made to address CVE-2016-5195.
PAN-68034	The show netstat CLI command was removed in the 7.1 release for Panorama, Panorama log collector, and WildFire. With this fix, the show netstat 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 (<i>all_pktproc</i>) stopped responding because a race condition occurred when closing sessions.
PAN-67639	Fixed an issue where the firewall did not properly mask the Auth Password and Priv Password for an SNMPv3 server profile (Device > Server Profiles > SNMP Trap) when you viewed the configuration change in a 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 where the firewall discarded SSL sessions when the server certificate chain size exceeded 23KB.
PAN-66873	Fixed an issue where PAN-OS deleted critical content files when the management plane ran out of memory, which caused commit failures until you updated or reinstalled the content.
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-65918	Fixed an issue on the Panorama virtual appliance where the third-party backup software BackupExec failed to back up a <i>quiesced</i> snapshot of Panorama (Panorama in a temporary state where all write operations are flushed). With this fix, the VMware Tools bundled with Panorama supports the quiescing option.

Issue ID	Description
PAN-64981	Fixed an issue where an internal buffer could be overwritten, causing the management plane to stop responding.
PAN-64884	Fixed an issue where firewalls in an HA configuration did not synchronize the Layer 2 MAC table; after failover, the MAC table was rebuilt only on the peer that became active, which caused excessive packet flooding.
PAN-64870	Fixed an issue where a zone with the Type set to Virtual Wire (Network > Zones) dropped all incoming traffic when you configured the Zone Protection profile for that zone with a Strict IP Address Check (Network > Network Profiles > Zone Protection > Packet Based Attack Protection > IP Drop) .
PAN-64723	Fixed an issue where the test authentication 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.
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 PA-7000 Series firewalls in an HA configuration where the NPC 40Gbps (QSFP) Ethernet interfaces on the passive peer displayed link activity on a neighboring device (such as a switch) to which they connected even though the interfaces were down on the passive peer.

Issue ID	Description
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 establishing an LDAP connection over a slow or unstable connection caused commits to fail when you enabled TLS. With this fix, if you enable TLS, the firewall does not attempt to establish LDAP connections when you perform a commit.
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 show high-availability path-monitoring command always showed the NPC as slot 1 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

Issue ID	Description
	SHA1/SHA256. With this fix, the firewall provides support for the SHA384 signature algorithm for client-based authentication.
PAN-61877	Fixed an issue where Authentication Override 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.
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 SYN Cookies action (Network > Zone Protection > Flood Protection).
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-61682	Fixed an issue where end users either did not see the Captive Portal web form or saw a page displaying raw HTML code after requesting an application through a web proxy because the HTTP body content length exceeded the specified size in the HTTP Header Content-Length.
PAN-61465	Fixed an issue where the web interface (Objects > Decryption Profile > SSL Decryption > SSL Protocol Settings > Encryption Algorithms) still displayed the 3DES encryption algorithm as enabled even after you disabled it.
PAN-61365	Fixed an issue where data filtering logs (Monitor > Logs > Data Filtering) 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 (upload, download, or both) in Objects > Security Profiles > Data Filtering and select the Direction column in Monitor > Logs > Data Filtering 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-

Issue ID	Description
	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 (File not found) 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	Fixed an issue where an application filter with no categories selected caused the firewall to perform slowly because the filter defaulted to include all categories (Objects > Application Filters). With this fix, you cannot configure an application filter without selecting one or more categories.
PAN-60556	<p>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.</p> <p>The OCSP Verify CA field in the certificate profile has been changed to OCSP Verify Certificate.</p>
PAN-60402	Fixed an issue where renaming an address object caused the commit to a Device Group to fail.
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.

Issue ID	Description
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	<p>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:</p> <pre data-bbox="537 911 1456 1213">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-58358	Fixed an issue where CSV exports for Unified logs (Monitor > Logs > Unified) displayed information in the wrong columns.
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

Issue ID	Description
	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 ifHCOctets 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-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-50038	Fixed an issue where the maximum transmission unit (MTU) size on the interfaces did not increase as expected when you enabled jumbo frames on a VM-Series firewall in AWS using the set deviceconfig setting jumbo-frame mtu configuration mode CLI command (the MTU on each interface remained at a maximum value of 1,500 bytes).
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.
PAN-40842	<p>Fixed a cosmetic issue where, when you configured a firewall to retrieve a WildFire signature package, the System log showed unknown version for that package. For example, after a scheduled WildFire package update, the System log showed:</p> <pre>WildFire package upgraded from version <unknown version> to 38978-45470.</pre>

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 PAN-OS® 8.0 documentation on the [Technical Documentation portal](#) using the links below. You can also [search](#) the documentation for more information on our products.

- [PAN-OS 8.0 New Features Guide](#)—Detailed information on configuring the features introduced in this release.
- [PAN-OS 8.0 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 8.0 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 8.0 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 8.0 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 8.0 Administrator's Guide](#)—Describes how to set up and manage GlobalProtect™ features.
- [PAN-OS 8.0 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>.

You can also use the Palo Alto Networks® [Contact Information](#) as needed.

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

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

