



PAN-OS® 6.1 Release Notes

Release 6.1.17

Revision Date: April 28, 2017

Review important information about Palo Alto Networks PAN-OS 6.1 software, including new features introduced, workarounds for open issues, and issues that are addressed in the PAN-OS 6.1 release. For installation, upgrade, and downgrade instructions, refer to the [PAN-OS 6.1 New Features Guide](#). For the [latest version of these release notes](#), refer to the Palo Alto Networks [technical documentation portal](#).

PAN-OS 6.1 Release Information	3
Features Introduced in PAN-OS 6.1	5
Management Features	5
WildFire Features	7
URL Filtering Features	9
Virtualization Features	9
Policy Features	10
GlobalProtect Features	10
High Availability (HA) Features	11
Networking Features	11
Changes to Default Behavior	13
Associated Software Versions	14
Known Issues	15
PAN-OS 6.1.17 Addressed Issues	21
PAN-OS 6.1.16 Addressed Issues	23
PAN-OS 6.1.15 Addressed Issues	25
PAN-OS 6.1.14 Addressed Issues	27
PAN-OS 6.1.13 Addressed Issues	29
PAN-OS 6.1.12 Addressed Issues	31
PAN-OS 6.1.11 Addressed Issues	33

PAN-OS 6.1.10 Addressed Issues35

PAN-OS 6.1.9 Addressed Issues37

PAN-OS 6.1.8 Addressed Issues41

PAN-OS 6.1.7 Addressed Issues45

PAN-OS 6.1.6 Addressed Issues51

PAN-OS 6.1.5 Addressed Issues55

PAN-OS 6.1.4-h2 Addressed Issues63

PAN-OS 6.1.4 Addressed Issues65

PAN-OS 6.1.3 Addressed Issues71

PAN-OS 6.1.2 Addressed Issues77

PAN-OS 6.1.1 Addressed Issues83

PAN-OS 6.1.0 Addressed Issues89

Getting Help.....97

 Related Documentation.....97

 Requesting Support98

PAN-OS 6.1 Release Information

This release note provides important information about Palo Alto Networks PAN-OS 6.1 software, including an overview of new features introduced in this release and a list of known issues. For instructions on how to [upgrade the firewall to PAN-OS 6.1](#) and configure the new features, refer to the [New Features](#) guide.

For the most up-to-date information, refer to the online version of the [PAN-OS 6.1 Release Notes](#) on the [Technical Documentation](#) portal.

▲ [Features Introduced in PAN-OS 6.1](#)

▲ [Changes to Default Behavior](#)

▲ [Associated Software Versions](#)



The Panorama certificate used to authenticate Panorama-to-firewall communication expires on June 16, 2017. Review [the most current information](#) about how to make sure you can continue using Panorama to manage firewalls and to aggregate firewall logs on Log Collectors after June 16, 2017:

<https://live.paloaltonetworks.com/t5/General-Topics/Panorama-Certificate-Expiration-on-June-16-2017/m-p/150948/thread-id/50050>. (Physical and virtual firewalls, WF-500 appliances, and M-500 appliances running in PAN-DB mode do not require any action.)



Starting with PAN-OS 6.1.15, all unresolved known issues and any newly addressed issues in these release notes are identified using new issue ID numbers that include a product-specific prefix. Issues addressed in earlier releases and any associated known issue descriptions continue to use their original issue ID.

▲ [Known Issues](#)

▲ [PAN-OS 6.1.17 Addressed Issues](#)

▲ [PAN-OS 6.1.16 Addressed Issues](#)

▲ [PAN-OS 6.1.15 Addressed Issues](#)

▲ [PAN-OS 6.1.14 Addressed Issues](#)

▲ [PAN-OS 6.1.13 Addressed Issues](#)

▲ [PAN-OS 6.1.12 Addressed Issues](#)

▲ [PAN-OS 6.1.11 Addressed Issues](#)

▲ [PAN-OS 6.1.10 Addressed Issues](#)

▲ [PAN-OS 6.1.9 Addressed Issues](#)

▲ [PAN-OS 6.1.8 Addressed Issues](#)

▲ [PAN-OS 6.1.7 Addressed Issues](#)

▲ [PAN-OS 6.1.6 Addressed Issues](#)

▲ [PAN-OS 6.1.5 Addressed Issues](#)

▲ [PAN-OS 6.1.4-h2 Addressed Issues](#)

▲ [PAN-OS 6.1.4 Addressed Issues](#)

▲ [PAN-OS 6.1.3 Addressed Issues](#)

▲ [PAN-OS 6.1.2 Addressed Issues](#)

- ▲ [PAN-OS 6.1.1 Addressed Issues](#)
- ▲ [PAN-OS 6.1.0 Addressed Issues](#)
- ▲ [Getting Help](#)

Features Introduced in PAN-OS 6.1

The following topics describe the new features introduced in the PAN-OS 6.1 release, which requires content release version 454 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 6.1 New Features Guide](#). The new features guide also provides additional information about how to use the new features in this release.

- ▲ [Management Features](#)
- ▲ [WildFire Features](#)
- ▲ [URL Filtering Features](#)
- ▲ [Virtualization Features](#)
- ▲ [Policy Features](#)
- ▲ [GlobalProtect Features](#)
- ▲ [High Availability \(HA\) Features](#)
- ▲ [Networking Features](#)

Management Features

The following Management features are introduced in PAN-OS 6.1. For more details about these features and for instructions on configuring them, refer to [Management Features](#) in the [PAN-OS 6.1 New Features Guide](#).

New Management Feature	Description
Security Policy Rulebase Enhancements	<p>The security policy rulebase enhancements enable more streamlined control over intrazone (within a zone) and interzone (between zones) traffic. With these enhancements, you can now create rules that enable visibility and control over intrazone or interzone traffic for multiple zone pairs in a single rule rather than having to create separate rules for each pair. To enable this flexibility, a new Rule Type classification indicates whether the rule matches intrazone traffic, interzone traffic, or both intrazone and interzone (called universal) traffic. The default Rule Type is universal. When you upgrade to PAN-OS 6.1, all existing rules in your security rulebase will be converted to universal rules.</p> <p>In addition, the implicit default rules the firewall uses for handling intrazone and interzone traffic that doesn't match any other rules have now been exposed, allowing you to override select settings—including logging, action, and threat inspection settings—on these rules.</p>
App Scope Enhancements	<p>App Scope has been updated to allow for improved security and a lighter footprint. This change supports enhancements that enable you to:</p> <ul style="list-style-type: none"> • Export maps, charts and images (.png or .pdf); export requires a browser that supports HTML 5 • Zoom-in and out of charts • Toggle legend entries in a chart to select the data that is displayed on the screen

New Management Feature	Description
Authenticated NTP	You can now configure the firewall to authenticate time updates from the NTP server used to synchronize the firewall clock. You can enable Authenticated NTP to use symmetric key exchange (shared secrets) or autokey (public key cryptography) authentication. Use Authenticated NTP to prevent tampering with the firewall clock and resulting disruptions to logging and schedule-based policies and services.
Multiple M-100 Interfaces	The Panorama™ M-100 appliance now supports the use of separate interfaces for management, device log collection, and collector group communication. Configure the eth0 (MGT), eth1, and eth2 interfaces interchangeably for one, two or all three functions. By default, the MGT interface performs all three functions but configuring separate interfaces is a best practice to improve security, control traffic prioritization, performance, and resilience.
Related Log Detail View Enhancements	To make it easier to correlate log information from a session, you can now click through the related logs in the Detailed Log View without closing the window and switching views. You can switch between the URL Filtering, Threat, Traffic, and Data Filtering logs associated with a session and the Detailed Log View window will dynamically update to display pertinent information for the selected log.
Log Forwarding Optimization	Log Forwarding has been enhanced to be more efficient and to use less CPU on all platforms.
Configurable Key Size for SSL Forward Proxy Server Certificates	<p>The firewall now supports both 2048-bit RSA keys (with SHA-256 hashing) and 1024-bit RSA keys (with SHA-1 hashing) for generating the certificates it uses to establish the SSL Forward Proxy session between itself and the client. This is an extension of the 2048-bit key support that was already available with SSL decryption. In previous releases, 2048-bit keys were supported in SSL Inbound Inspection sessions as well as in SSL Forward Proxy sessions between the firewall and the destination server.</p> <p>As part of the extended support for 2048-bit keys, the firewall will now by default dynamically choose the key size to use to establish SSL Forward Proxy sessions with clients, based on the key size used by the destination server. You can optionally configure a static key size for SSL Forward Proxy sessions between the firewall and clients regardless of the key size used by the destination server.</p>
Default profile group and log forwarding settings	You can now allow new security policies and new security zones to include your organization's preferred settings for security profile groups or log forwarding by default. Create a default security profile group or default log forwarding profile ; the default profile group will be attached to new security policies automatically and the default log forwarding profile will be selected for new security policies and new security zones automatically. With a default security profile group and a default log forwarding profile configured, you can quickly create new security policies and security zones without manually selecting your preferred settings for log forwarding or a profile group each time. This also allows you to enforce consistency for other administrators creating new policy rules or zones, by including your organization's preferred profile group and log forwarding options in new policies or zones automatically.

WildFire Features

The following WildFire™ features are introduced in PAN-OS 6.1. For more details about these features and for instructions on configuring them, refer to [WildFire Features](#) in the [PAN-OS 6.1 New Features Guide](#).

New WildFire Feature	Description
Signature/URL Generation on the WildFire Appliance	<p>The WF-500 appliance can now generate signatures locally, eliminating the need to send any data to the public cloud in order to block malicious content. The WF-500 WildFire appliance can now analyze files forwarded to it from Palo Alto Networks firewalls or from the WildFire API and generate the following types of signatures that block both the malicious files as well as associated command and control traffic:</p> <ul style="list-style-type: none"> • Antivirus signatures detect and block malicious files. These signatures are added to WildFire and Antivirus content updates. • DNS signatures detect and block callback domains for command and control traffic associated with malware. These signatures are added to WildFire and Antivirus updates. • URL Categorization classifies callback domains as malware and updates the URL category in PAN-DB. <p>Firewalls must be running PAN-OS 6.1 or later to enable local signature generation for forwarded files. In addition, you must configure the firewalls to receive content updates from the WF-500 WildFire appliance, which can occur as frequently as every five minutes. You can optionally send the malware sample file analysis data (or just the XML report if you don't want to send the sample) to the WildFire public cloud to enable signature generation for distribution through the Palo Alto Networks update server.</p>
Content Updates on the WF-500 WildFire Appliance	<p>To support the ability to generate signatures on the local WF-500 WildFire appliance, daily content updates are now available for the appliance. These content updates equip the appliance with the most up-to-date threat information for accurate malware detection and improve the appliance's ability to differentiate the malicious from the benign.</p>
Email Header Information in WildFire Logs	<p>The firewall now captures email header information—email sender, recipient and subject—and sends it along with the corresponding email attachments and email links that it forwards to WildFire. If WildFire determines that the email attachment or link is malicious, it includes the email header information in the WildFire Submissions log that it returns to the firewall. This information can help you quickly track down and remediate threats that are detected in emails received by your users. Note that neither the firewall nor WildFire receive, store, or view the actual email contents.</p>
Flash and Office Open XML File Type Support	<p>Firewalls can now forward Flash content embedded in web pages to WildFire for analysis. In addition, WildFire now creates antivirus signatures for Flash applets and Office Open XML (OOXML) 2007+ documents that it determines to be malicious and delivers the signatures through antivirus updates, enabling you to alert or block malicious content in these types of files. To support this capability, the firewall must have a WildFire subscription and be running Content Release version 454 or later.</p>

New WildFire Feature	Description
WildFire Email Link Analysis	<p>The firewall can now extract HTTP/HTTPS links contained in SMTP and POP3 email messages and forward the links to the WildFire public cloud for analysis (this feature is not supported on the WF-500 WildFire appliance). Enable this functionality by configuring the firewall to forward the email-link file type. Note that the firewall only extracts links and associated session information (sender, recipient, and subject) from the email messages that traverse the firewall; it does not receive, store, forward, or view the email message. After receiving an email link from a firewall, WildFire visits the links to determine if the corresponding web page hosts any exploits. If it detects malicious behavior on the page, it returns a malicious verdict and:</p> <ul style="list-style-type: none"> • Generates a detailed analysis report and logs it to the WildFire Submissions log on the firewall that forwarded the links. This log now includes the email header information-email sender, recipient and subject-so that you can identify the message and delete it from the mail server and/or track down the recipient and mitigate the threat if the email has already been delivered and/or opened. • Adds the URL to PAN-DB and categorizes it as malware. <p>Note that if the link corresponds to a file download, WildFire does not analyze the file. However, the firewall will forward the corresponding file to WildFire for analysis if the end user clicks the link to download it as long as the corresponding file type is enabled for forwarding. Note also that WildFire does not send a log to the firewall if it determines a link to be benign even if you have enabled logging of benign files because of the large number of logs this would generate.</p>
WildFire Analysis Report Enhancements	<p>The WildFire detailed report provides new forensic details to help you quickly identify threat severity and signature coverage status:</p> <ul style="list-style-type: none"> • The report now provides details about each behavior that the sample file exhibits and the corresponding Severity of each behavior. A visual gauge provides an at-a-glance indicator of severity level; one bar indicates low severity and each additional bar indicates a higher severity level. • A new Coverage Status section dynamically updates when the report is rendered on the firewall. This section displays up-to-date information about what signature and URL filtering coverage that Palo Alto Networks currently provides to protect against the threat.
Windows 7 64-bit Support	<p>WildFire now supports the Microsoft Windows 7 64-bit sandbox environment on both the WildFire public cloud and the WF-500 WildFire appliance. Support for this environment on the WF-500 appliance requires that you upgrade the appliance OS to 6.1 and install the Windows 7 64-bit image.</p>
WildFire XML API Support on the WildFire Appliance	<p>The WF-500 appliance now supports the WildFire XML API. To use WildFire XML API with the appliance, you must generate the API key on the appliance. The WF-500 appliance supports up to 100 API keys.</p>

URL Filtering Features

The following URL Filtering features are introduced in PAN-OS 6.1. For more details about these features and for instructions on configuring them, refer to [URL Filtering Features](#) in the [PAN-OS 6.1 New Features Guide](#).

New URL Filtering Feature	Description
Logging of HTTP Header Fields	To facilitate troubleshooting and forensic analysis, you can now enable logging of one or more of the following HTTP header fields in the URL Filtering profile: User-Agent, Referer, and X-Forwarded-For. The HTTP header information for each matching session will be included in the URL Filtering logs, and will also be displayed in a new widget in the Detailed Log View for URL Filtering, Threat, and WildFire logs. The HTTP header fields in URL filtering logs are also available for custom log forwarding to a syslog server and for inclusion in custom reports on the firewall and on Panorama.
Manual Upload of BrightCloud Database	In deployments where Panorama or a firewall has no direct Internet access, you can now manually upload and install the BrightCloud database .
Full-path Categorization of URLs in PAN-DB	PAN-DB can now categorize content down to the page level instead of just at the directory level. Because the pages within a domain can belong to multiple categories, this capability provides increased accuracy in filtering content and prevents potential over-blocking of web content. If, for example, you block malware and allow access to business/ news content for users on your network, they can access http://www.acme.com/c/news.html because it is categorized as news/business, but be denied access to http://www.acme.com/c/malware.exe because PAN-DB categorizes the full-path for this web page as malware. To test the category for a full path of a valid URL, use https://urlfiltering.paloaltonetworks.com/testASite.aspx .

Virtualization Features

The following Virtualization features are introduced in PAN-OS 6.1. For more details about these features and for instructions on configuring them, refer to [Virtualization Features](#) in the [PAN-OS 6.1 New Features Guide](#).

New Virtualization Feature	Description
Support for VM-Series on Amazon Web Services (AWS)	<p>If you are moving or have moved your servers/applications from self-managed datacenters to a Virtual Private Cloud (VPC) within the Amazon Web Services (AWS) cloud, you can now deploy the VM-Series firewall as a secure gateway to your VPC. The VM-Series firewall is available as a public Amazon Machine Image (AMI) and can be deployed on an Elastic Compute Cloud (EC2) instance. Consistent with the Amazon AWS networking requirements, VM-Series firewalls deployed in the Amazon AWS support only Layer 3 interfaces.</p> <p>In addition, the VM Information Sources feature in PAN-OS software has been extended to monitor changes in the AWS VPC. Using the VM Information Sources feature, the firewall can connect to an Amazon VPC and collect EC2 instance IP addresses and associated metadata as tags to gain context awareness, which then allows for consistent security policy enforcement despite changes in the EC2 instance inventory.</p>

New Virtualization Feature	Description
Support for VM-Series on Kernel-based Virtual Machine (KVM)	The VM-Series firewall can be installed on 64-bit versions of Linux distributions running KVM hypervisor deployed on x86 hardware with Intel or AMD chipsets with virtualization extensions enabled. The supported Linux distributions are CentOS, Red Hat Enterprise Linux (RHEL), and Ubuntu. VM-Series firewalls deployed on KVM support e1000, virtio, PCI passthrough, and Single Root I/O Virtualization (SR-IOV) network drivers.

Policy Features

The following Policy feature is introduced in PAN-OS 6.1.7. For more details about this feature and for instructions on configuring it, refer to the [PAN-OS 6.1 Administrator's Guide](#).

New Policy Feature	Description
DoS Protection Against Flooding of New Sessions	In PAN-OS 6.1.7 and later 6.1 releases (and in PAN-OS 7.0.2 and later releases), you can configure DoS protection to better block IP addresses to handle high-volume single-session and multiple-session attacks more efficiently. For configuration details, see DoS Protection Against Flooding of New Sessions .

GlobalProtect Features

The topics in this section are the new GlobalProtect™ features introduced in PAN-OS 6.1. For more details about these GlobalProtect features and for instructions on configuring them, refer to [GlobalProtect Features](#) in the [PAN-OS 6.1 New Features Guide](#).

For information on related features introduced in the GlobalProtect Mobile Security Manager 6.1 release, including how to set up an enterprise app store for your users and how to isolate business traffic and data on mobile devices, refer to the [GlobalProtect Mobile Security Manager 6.1 New Features Guide](#).

New GlobalProtect Feature	Description
Extended SSO Support for GlobalProtect Agents	With Single Sign-On (SSO) , the GlobalProtect agent wraps the user's Windows login credentials to automatically authenticate and connect to the GlobalProtect portal and gateway. SSO has been enhanced in this release so that when a third-party credential provider is being used to wrap the user's Windows login credentials, the GlobalProtect agent wraps the third-party credentials to allow for successful authentication for the Windows user. This extended SSO functionality is supported on Windows 7 and Windows Vista clients.
Per App VPN for GlobalProtect iOS App	The GlobalProtect iOS app now supports Per App VPN . With Per App VPN enabled, the GlobalProtect iOS app will route all traffic from managed business apps through your corporate VPN, while personal apps that are not managed can connect directly to the Internet. An MDM service, such as the GlobalProtect Mobile Security Manager, is required to enable the GlobalProtect iOS app's per App VPN capability.

New GlobalProtect Feature	Description
Disconnect on Idle	The options to time out GlobalProtect clients have been extended to include settings you can use to log out idle users . You can set the number of minutes after which users will be disconnected from GlobalProtect if there is no traffic going through the VPN.
Disable Browser Access to the Portal Login Page	Prevent public access to the GlobalProtect portal login page and unauthorized attempts to authenticate to the GlobalProtect portal from a web browser by disabling the portal login page . With the portal login page disabled, you can use a software distribution tool, such as Microsoft's System Center Configuration Manager (SCCM), to allow your users to download and install the GlobalProtect agent. GlobalProtect agents and apps will continue to successfully authenticate and connect to the portal to receive configuration updates.

High Availability (HA) Features

The following HA feature is introduced in PAN-OS 6.1.7. For more details about this feature and for instructions on configuring it, refer to the [PAN-OS 6.1 Administrator's Guide](#).

New High Availability Feature	Description
HA Session Sync During Upgrade from One Feature Release to the Next	<p>Session syncing will now remain operable when upgrading HA peers from one PAN-OS feature release version to the next feature release version (for example, when upgrading the firewalls from PAN-OS 6.0.x to PAN-OS 6.1.x). Although session syncing has always been operable when upgrading from one maintenance release to another in the same feature release version (for example, during upgrade from PAN-OS 6.0.1 to PAN-OS 6.0.3), in prior releases it was inoperable when upgrading from one PAN-OS feature release to the next. This meant that if there was a failover during the period of time when the individual firewalls in the HA pair were running different feature release versions (for example, if one firewall was running 5.0.13 and the other one was running 6.0.3) sessions could have been impacted.</p> <p>VM-Series firewall and the PA-200, only support HA lite without session synchronization capability.</p>

Networking Features

The following Networking features are introduced in PAN-OS 6.1. For more details about these features and for instructions on configuring them, refer to [Networking Features](#) in the [PAN-OS 6.1 New Features Guide](#).

New Networking Feature	Description
NAT Enhancement for Session Load Balancing	On PA-5000 Series platforms, Static Source NAT, Dynamic IP NAT, and Destination NAT session processing has been enhanced to allow the firewall to use multiple CPUs to process NAT sessions, rather than anchoring the sessions to a CPU based on destination IP hash. This enhancement greatly improves throughput in these NAT scenarios, particularly in topologies that include a load balancer or other device that limits the number of destination IP addresses. This enhancement will occur automatically upon upgrade of the PA-5000 Series device. Note that Dynamic IP and Port NAT (DIPP) or Dynamic IP NAT sessions that fall back to DIPP will continue to be anchored to a specific CPU based on the destination IP address (the target translated address).
NAT Capacity Enhancements	The maximum number of NAT rules (static, Dynamic IP, and Dynamic IP/Port) allowed for each platform has been increased and NAT statistics now include usage and memory information to provide efficient management of NAT rules. The Dynamic IP/Port oversubscription ratio can now be tuned to allow greater control in environments requiring more Dynamic IP and Dynamic IP/Port rules. These NAT capacity enhancements are supported on PA-3000 Series, PA-4000 Series, PA-5000 Series, and PA-7050 platforms.
LACP	You can now use the Link Aggregation Control Protocol (LACP) to dynamically detect the interfaces between interconnected devices (peers) and combine those interfaces into an aggregate group. Enabling LACP provides redundancy within an aggregate group: the protocol automatically detects interface failures and fails over to standby interfaces. LACP is supported on Layer 2, Layer 3, and HA3 interfaces only and is supported on PA-500, PA-3000 Series, PA-4000 Series, PA-5000 Series and PA-7050 platforms.
Remove TCP Timestamp	A new Remove TCP Timestamp option has been added to the Zone Protection profile to enable you to strip the TCP timestamp from the TCP header. This option is available in the web interface and in the CLI.
TCP Session Closing Timers	<p>Two new timers have been added (TCP Time Wait and TCP Unverified RST) and the tcp-wait timer has been renamed the TCP Half Closed timer, as detailed below:</p> <ul style="list-style-type: none"> The TCP session termination procedure now has a TCP Half Closed timer, which is triggered by the first FIN the firewall sees for a session, and a second timer (TCP Time Wait), which is triggered by the second FIN or a RST. You can set these timers globally or per application. In prior releases, only one TCP wait timer existed, triggered by the first FIN. If that setting was too short, the half-closed sessions could be closed prematurely. Conversely, a setting that was too long could make the session table grow too much and possibly use up all of the sessions. By having two timers, a relatively long TCP Half Closed timer allows the opposite side time to respond, and a short TCP Time Wait timer quickly ages fully closed sessions and controls the size of the session table. A TCP Unverified RST timer has been added at the global level. If the firewall receives a RST that cannot be verified (because it has an unexpected sequence number within the TCP window or it is from an asymmetric path), the TCP Unverified RST timer controls the aging out of the session. This timer provides an additional security measure.
Session End Reason Logging	When troubleshooting connectivity and application availability issues, knowing what caused a session to terminate can be useful. PAN-OS now provides a new session end reason field in traffic logs. Session end reasons can also be included in reports that are generated based on traffic logs and SNMP traps and email alerts that are triggered by traffic logs contain session end reasons, as well.

Changes to Default Behavior

The following are changes to default behavior in PAN-OS 6.1:

Feature	Change
Decryption	The default key size for SSL/TLS Forward Proxy certificates has changed from 1024-bit RSA to Defined by destination host . The new default setting allows PAN-OS to generate certificates based on the destination server's key.
Security policy	A new Rule Type classification indicates whether a security rule matches intrazone traffic, interzone traffic, or both (<i>universal</i>). In releases prior to PAN-OS 6.1, the rule type classification did not exist and all rules were considered universal. Existing rules in the rulebase are converted to universal rules when you upgrade to PAN-OS 6.1; you can then choose to change the Rule Type to intrazone or interzone or you can choose to leave it classified as universal .
GlobalProtect	The GlobalProtect agent now collects the domain that is defined for the <code>ComputerNameDnsDomain</code> parameter from Windows clients. This is the DNS domain assigned to the local computer or the cluster associated with the local computer. The value for the <code>ComputerNameDnsDomain</code> parameter determines the Domain displayed in the HIP Match logs for Windows clients.

Associated Software Versions

The following minimum software versions are supported with PAN-OS 6.1. To see a list of the next-gen firewall models that support PAN-OS 6.1, see the [Palo Alto Networks® Compatibility Matrix](#).

Palo Alto Networks Software	Minimum Supported Version with PAN-OS 6.1
Panorama™	6.1.0
User-ID™ Agent	6.0.0
Terminal Services Agent	5.0.0
NetConnect	Not supported in 6.1
GlobalProtect™ Agent	1.2.0
GlobalProtect Mobile Security Manager	6.0.0
Content Release Version	454

Known Issues

The following list describes known issues in the PAN-OS 6.1 release:




Starting with PAN-OS 6.1.15, all unresolved known issues and any newly addressed issues in these release notes are identified using new issue ID numbers that include a product-specific prefix. Issues addressed in earlier releases and any associated known issue descriptions continue to use their original issue ID.



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>.

Issue Identifier	Issue Description
PAN-67072	In PAN-OS 6.1 and 7.0, the firewall applies the wrong security policy if a user attempts to download a blocked file by selecting Resume in the blocked page dialog presented by the browser, allowing the user to download the blocked file. This issue occurs when a security policy that blocks downloads has a lower priority than a security policy that applies an action such as URL filtering (but does not block downloads) on the same traffic. This issue is resolved in PAN-OS 7.1 and later releases. Workaround: Change the order of the security policies so that the download-blocking policy has a higher priority than the URL-filtering policy.
PAN-61724 (101293)	The Network Monitor report (Monitor > App Scope > Network Monitor) displays only partial data when you select Source or Destination for a data set that includes a large number of source or destination IP addresses and usernames. However, the report does display all data as expected when you instead select Application or Application Category for a large data set.
102159	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 results in issues after the firewall is powered on again. Refer to Issue 1332563 in the VMware release notes: www.vmware.com/support/pubs/nsx_pubs.html 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.
98112 <i>This issue is now resolved. See PAN-OS 6.1.13 Addressed Issues.</i>	Fixed an issue with firewalls in an HA active/active configuration where session timeouts for some traffic were unexpectedly refreshed after a commit or HA sync attempt.
97806	For firewalls running PAN-OS 6.1.12 in an HA active/active configuration, the peer that is not the session owner intermittently incorrectly ages out sessions, which results in the premature removal of those sessions from both peers.
93078	HA session synchronization between peers will fail if one peer is running PAN-OS 6.1.6 or an earlier release while the other is running PAN-OS 6.1.7 or a later release. The resulting incomplete session synchronization will cause dropped packets if a failover occurs when firewalls are passing traffic while in this configuration. Workaround: If upgrading an HA peer from PAN-OS 6.1.6 (or an earlier release) to PAN-OS 6.1.7 (or a later release), you should also upgrade the second peer as soon as possible to PAN-OS 6.1.7 or a later release to avoid dropped packets after a failover.

Issue Identifier	Issue Description
92423	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).
90256 <i>This issue is now resolved. See PAN-OS 6.1.12 Addressed Issues.</i>	Decrypted SSH sessions are not mirrored to the decrypt mirror interface as expected.
89385 <i>This issue is now resolved. See PAN-OS 6.1.12 Addressed Issues.</i>	<p>For a firewall in an HA active/active configuration, session timeouts for some traffic unexpectedly refresh after a commit or HA sync attempt.</p> <p> This fix introduced a known issue: 97806.</p>
86623	A firewall in an HA active/passive configuration with an established FTP session drops FTP PORT command packets after a failover.
84594	<p>On a PA-7050 firewall, one data port must be configured as a log card interface because the traffic and logging capabilities of this platform exceed the capabilities of the management port. A log card interface performs WildFire file-forwarding and log forwarding for syslog, email, and SNMP and these services require DNS support. If you have set up a custom service route for firewall DNS queries, services using the log card interface might not be able to generate DNS requests. This is only an issue if you've configured the firewall to use a service route for DNS requests, and in this case, you must perform the following workaround to enable communication between the firewall dataplane and the log card interface.</p> <p>Workaround: Enable the DNS Proxy on the firewall, and do not specify an interface for the DNS proxy object (leave the field Network > DNS Proxy > Interface clear). See the steps to enable DNS proxy or use the CLI command <code>set deviceconfig system dns-setting dns-proxy-object</code>.</p>
82605 <i>This issue is now resolved. See PAN-OS 6.1.9 Addressed Issues.</i>	<p>Offloaded policy-based forwarding (PBF) sessions will fail to egress a firewall running PAN-OS 6.1.4 and later releases if you Enforce Symmetric Return (Policies > Policy Based Forwarding > <pbf-rule> > Forwarding).</p> <p>Workaround: Disable Enforce Symmetric Return and create bidirectional PBF policies.</p>
81584 <i>This issue is now resolved. See PAN-OS 6.1.7 Addressed Issues.</i>	In Panorama 6.1.3 and later releases, output from the <code>show ntp</code> command does not always display the correct NTP status. This primarily occurs when there is only one NTP server configured where, even when correctly connected to the NTP server, the <code>show ntp status</code> displays as <code>rejected</code> .
76489	<p>Threat updates do not install correctly after adding a Threat Prevention license and installing an Applications and Threats content release version even though the output of the <code>show system info</code> CLI command confirms that the Threat Prevention license is installed.</p> <p>Workaround: Manually install a different Applications and Threats package or wait for the next content download.</p>
74180	On PA-7050 firewalls in HA configurations, a TCP connection cannot be established when you configure a virtual wire subinterface with VLAN tags and IP classifiers.

Issue Identifier	Issue Description
72715 <i>This issue is now resolved. See PAN-OS 6.1.4 Addressed Issues.</i>	An M-100 appliance in Panorama™ mode running PAN-OS 6.1.2 or PAN-OS 6.1.3 is unable to receive logs forwarded by a managed firewall. Workaround: check that all managed firewalls are assigned to a Log Collector (Panorama > Collector Groups > Device Log Forwarding). Assign a Log Collector to any managed firewalls that do not have a log forwarding preference configured.
71609 <i>This issue is now resolved. See PAN-OS 6.1.4 Addressed Issues.</i>	Special characters are not supported in the local portion of an email address (the text in front of @) for email addresses specified in email server profiles (Device > Server Profiles > Email). If you downgrade to a release earlier than PAN-OS 6.1.4, you should expect the following commit errors if there are special characters in the local portion of any email address in your email server profiles in your PAN-OS 6.1.4 or later release: <ul style="list-style-type: none"> • Pushing email addresses with special characters from PAN-OS 6.1.4 or higher releases to devices running PAN-OS 6.1.3 or earlier releases will fail. • Subsequent autocommit events after the initial autocommit initiated during the downgrade process to a PAN-OS 6.1.3 or earlier release will fail if email addresses in email server profiles contain special characters.
70222	If the password for the administrator's account on the NSX Manager contains special characters (such as "\$"), Panorama cannot communicate with the NSX Manager. The inability to communicate prevents context-based information, such as Dynamic Address Groups, from being available to Panorama. Workaround: Remove special characters from the password on the NSX Manager.
69725 <i>This issue is now resolved. See PAN-OS 6.1.1 Addressed Issues.</i>	A Log Collector running a PAN-OS 6.0 release does not correctly receive NTP server configuration settings when pushed from Panorama running 6.1.0. When both the Log Collector and Panorama are running 6.1.0, NTP server configuration settings can be successfully pushed from Panorama to the Log Collector.
69598 <i>This issue is now resolved. See PAN-OS 6.1.1 Addressed Issues.</i>	Autocommits can fail following an upgrade to PAN-OS 6.1.0 if Aggregate Ethernet (AE) interfaces have been previously configured without defining an interface type (this can only be an issue when using the CLI; the web interface requires the interface type to be defined). Before upgrading to PAN-OS 6.1.0, ensure that all AE interfaces are configured as a specific interface type: HA, Layer 2, Layer 3, or virtual-wire.
69458	When using a loopback interface as a GlobalProtect™ gateway, traffic is not routed correctly for third-party IPsec clients. Workaround: Use a physical interface instead of a loopback interface as the GlobalProtect gateway 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.
68588 <i>This issue is now resolved. See PAN-OS 6.1.1 Addressed Issues.</i>	If you configure a firewall as a Panorama-managed device but you do not restart the firewall after doing so, the firewall will forward predefined reports to Panorama that do not display any data. Workaround: To ensure that predefined reports forwarded to Panorama are populated correctly after configuring the firewall as a managed device, restart the management server in one of two ways: either reboot the firewall or execute the <code>debug software restart management-server</code> CLI command.
68484	On Panorama, if you disable the Share Unused Address and Service Objects with Devices setting and perform a device group commit, committing changes to a device group will not push address objects to managed firewalls as expected.

Issue Identifier	Issue Description
68330	When you configure a firewall to retrieve a WildFire signature package, the System log shows <code>unknown version</code> for the package. For example, after a scheduled WildFire package update, the system log shows: <code>wildfire package upgraded from version <unknown version> to 38978-45470</code> . This is a cosmetic issue only and does not prevent the WildFire package from installing.
68153	On a firewall with numerous interfaces, the scheduled and unscheduled (on demand) reports display discrepancies in the byte counts for traffic logs and the repeat counts for Threat and Data Filtering logs.
67713	PAN-OS allows downgrade to content release versions (Applications and Threats) on the firewall to versions that the current PAN-OS release does not support. For example, if the firewall is running PAN-OS 6.1.0 and the minimum content release version is 454, you should not be able to downgrade to a version earlier than 454.
67624	When using a web browser to view a WildFire Analysis Report from a firewall that is using a WF-500 appliance for file sample analysis, the report may not appear until the browser downloads the WF-500 certificate. This issue occurs after upgrading a firewall and the WF-500 appliance to a PAN-OS 6.1 or later release. Workaround: Browse to the IP address or hostname of the WF-500 appliance, which will temporarily download the certificate into the browser. For example, if the IP address of the WF-500 appliance is 10.3.4.99, open a browser and enter <code>https://10.3.4.99</code> . You can then access the report from the firewall by selecting Monitor > WildFire Submissions , clicking the log details icon, and then selecting the WildFire Analysis Report tab.
67552	Firewalls running PAN-OS 6.0 and earlier releases send a NIL value (“-” or en-dash) to the syslog server when no domain or hostname value is configured on the firewall. In PAN-OS 6.1 and later releases, the firewall does not send any value when the domain and hostname fields are empty; instead, this field is left blank in syslog headers.
66976	In the WildFire Submissions Logs, the email recipient address is not correctly mapped to a username when configuring mapping with group mapping profiles that are pushed in a Panorama template.
66887	The VM-Series firewall on KVM, for all supported Linux distributions, does not support the Broadcom network adapters for PCI pass-through functionality.
66879	The VM-Series firewall on KVM running on Ubuntu 12.04 LTS does not support PCI pass-through functionality.
66745	On managed mobile devices running iOS 8, unenrolling the device does not always remove the VPN and Mobile Security Manager profiles.
66233	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).
66059	Regardless of the Time Frame you specify for a scheduled custom report on a Panorama M-100 appliance, the earliest possible start date for the report data is effectively the date when you configured the report. For example, if you configure the report on the 15th of the month and set the Time Frame to Last 30 Days , the report that Panorama generates on the 16th will include only data from the 15th onward. This issue applies only to scheduled reports; on-demand reports include all data within the specified Time Frame . Workaround: To generate an on-demand report, click Run Now when you configure the custom report.

Issue Identifier	Issue Description
65824	<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 the new pools together exceed the memory limit.</p> <p>Workaround: Commit a second time, which clears the old pool allocation.</p>
<p>64658</p> <p><i>This issue is now resolved. See PAN-OS 6.1.5 Addressed Issues.</i></p>	<p>When setting up or modifying a DoS Protection profile, you can set a maximum number of concurrent sessions for traffic that matches the profile. The maximum concurrent limit of sessions for PAN-OS 6.1.0 through PAN-OS 6.1.4 releases is 65,535. After you upgrade to a PAN-OS 6.1.0 through PAN-OS 6.1.4 release, check that the Maximum Concurrent Sessions configured is less than 65,535 (Objects > DoS Protection > DoS Protection Profile > Resources Protection). You will not be able to commit configuration changes if the Maximum Concurrent Sessions field was set to a value higher than 65,535 while running a previous release version until after you enter a value for this field that is less than 65,535.</p>
63962	<p>Configurations pushed from Panorama 6.1 and later releases to firewalls running PAN-OS 6.0.3 or earlier PAN-OS 6.0 releases will fail to commit due to an <code>unexpected Rule Type</code> error. This issue is caused by the new Rule Type setting in Security policy rules that was not included in the upgrade transform and, therefore, the new rule types are not recognized on devices running PAN-OS 6.0.3 or earlier PAN-OS releases.</p> <p>Workaround: Only upgrade Panorama to version 6.1 or later releases if you are also planning to upgrade all managed firewalls running PAN-OS 6.0.3 or an earlier PAN-OS 6.0 release to a PAN-OS 6.0.4 or later release before pushing a configuration to the devices.</p>
<p>63854</p> <p><i>This issue is now resolved. See PAN-OS 6.1.5 Addressed Issues.</i></p>	<p>For PAN-OS 6.0 release versions, virtual system administrators can perform XML API configuration commands only for the virtual systems they are an administrator for and no longer have access to XML API operational mode commands.</p>
63524	<p>When you perform a template commit to a PA-200 firewall, the operation fails if you change the vsys1 display name on the firewall using the <code>set display-name <name></code> CLI command.</p> <p>Workaround: Leave the display name at its default value (vsys1); if already changed, reset it to the default value.</p>
63186	<p>If you perform a factory reset on a Panorama virtual appliance and configure the serial number, logging does not work until you reboot Panorama or execute the <code>debug software restart management-server</code> CLI command.</p>
61720	<p>By default, the GlobalProtect app adds a route on iOS mobile devices that causes traffic to the MDM server 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 MDM server—to pass through the VPN tunnel, perform the following tasks on the firewall hosting the GlobalProtect gateway (Network > GlobalProtect > Gateways > Client Configuration > Network Settings > Access Route):</p> <ul style="list-style-type: none"> • Add <code>0.0.0.0/0</code> as an access route. • Enter the IP address for the MDM server as an additional access route.
60851	<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>

Issue Identifier	Issue Description
59856	<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 reconnect 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 active Panorama peer synchronizes the configuration. During this time, the passive Panorama peer will log a critical message: <code>vm-cfg: failed to process registration from svm device. vm-state: active</code>. This message is logged until you commit the changes on the active Panorama, which then initiates synchronization between the Panorama HA peers so that 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 an HA setup, the commit will initiate the synchronization of the running configuration between the Panorama peers.</p>
59573	<p>Live migration of the VM-Series firewall is not supported when you enable SSL decryption using the forward proxy method. Use SSL inbound inspection if you need support for live migration.</p>
58839	<p>When deleting the VM-Series deployment, all VMs are deleted successfully; however, sometimes a few instances still remain in the datastore.</p> <p>Workaround: Manually delete the VM-Series firewalls from the datastore.</p>
58260	<p>If an HA failover occurs on Panorama at the time that the NSX Manager is deploying the VM-Series NSX edition firewall, the licensing process fails with the error: <code>vm-cfg: failed to process registration from svm device. vm-state: active</code>.</p> <p>Workaround: Delete the unlicensed instance of the VM-Series firewall on each ESXi host and then redeploy the Palo Alto Networks next-generation firewall service from the NSX Manager.</p>
58202	<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 Filter menu 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 the global (or browser) refresh option.</p>
49742	<p>The following issues apply when configuring a firewall to use a hardware security module (HSM):</p> <ul style="list-style-type: none"> • Thales nShield Connect—The firewall requires at least four minutes to detect that an HSM has been disconnected, causing SSL functionality to be unavailable during the delay. • SafeNet Network—When losing connectivity to either or both HSMs in an HA configuration, the display of information from the <code>show ha-status</code> and <code>show hsm info</code> commands is blocked for 20 seconds.
49322	<p>After you configure Panorama M-100 appliances for high availability and synchronize the configuration, the Log Collector of the passive peer cannot connect to the active peer until you reboot the passive peer.</p>
40436	<p>Firewalls running PAN-OS 6.1 and later releases do not update FQDN entries unless you enable the DNS proxy Cache option (Network > DNS Proxy > <DNS Proxy config> > Advanced).</p>

PAN-OS 6.1.17 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.17 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
PAN-74735	Fixed an issue where the server certificate that Panorama used to authenticate communications with other devices did not comply with new Common Criteria Network Device collaborative Protection Profile (NDcPP) requirements. This fix replaces the server certificate with one that has the X509v3 extensions required for NDcPP compliance, including Basic Constraints, Key Usage, Extended Key Usage, and the Authority Key Identifier. Furthermore, with this fix, the client certificates generated on Panorama will also include the Extended Key Usage extension.
PAN-74222	Fixed an issue where the PA-7050 firewall allowed you to downgrade to a PAN-OS release that did not support a Switch Management Card (SMC) running hardware version 2.0, which resulted in an SMC slot failure after the downgrade. With this fix, a PA-7050 firewall with a version 2.0 SMC does not let you downgrade to a release earlier than PAN-OS 6.1.
PAN-73045	Fixed an issue where HA failover and fail-back events terminated sessions that started before the failover.
PAN-72769	A security-related fix was made to prevent brute-force attacks on the GlobalProtect external interface (CVE-2017-7945).
PAN-71073	Fixed an issue where a commit associated with a dynamic update caused an HA failover when the path-monitoring target IP address aged out or when the first path-monitoring health check failed.
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-69801	Fixed an issue where the primary firewall peer in an HA active/active configuration was in a tentative HA state and did not synchronize session update messages with the secondary peer, which resulted in dropped packets after a session aged out (within 30 seconds).
PAN-68431	Fixed an issue where firewalls and Panorama failed to send SNMPv3 traps if you configured the service route to forward the traps over a dataplane interface.
PAN-62159	Fixed an issue where the firewall did not generate WildFire Submissions logs when the number of cached logs exceeded storage resources on the firewall.

Issue Identifier	Issue Description
PAN-62015	Fixed an issue on PA-7000 Series firewalls where, when creating the key for a GRE packet, the firewall did not use the same default values for the source and destination ports in the hardware and software, which slowed the firewall performance.
PAN-59677	Fixed an issue where the firewall allowed administrators logged in as root to use GNU Wget to access remote servers and write to arbitrary files by redirecting a request from HTTP to a crafted FTP resource.
PAN-58589	Fixed an issue where the dataplane restarted when a process (<i>pan_comm</i>) experienced an out-of-memory condition.
PAN-57520	Fixed an issue where firewalls stopped connecting to Panorama when the root CA server certificate on Panorama expired. With this fix, Panorama replaces the original certificate with a new certificate that expires in 2024.
PAN-46374	Fixed an issue on the PA-7050 firewall where the Switch Management Card (SMC) did not come up following a soft reboot (such as after upgrading the PAN-OS software); power cycling was required to bring up the SMC.
PAN-41288	Fixed an issue where the management server process (<i>mgmtsvr</i>) stopped running due to corrupt LLDP type-length-value (TLV) elements.

PAN-OS 6.1.16 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.16 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
PAN-73605	Fixed an issue where the firewall did not correctly identify the URL category of a web session when the HTTP header information was split across multiple packets due to a sequence of abnormally large HTTP cookies.
PAN-70428	A security-related fix was made to prevent inappropriate information disclosure to authenticated users (CVE-2017-5583).
PAN-68062	Fixed an issue where the firewall failed to apply the correct action if the vulnerability profile had a very long list of CVEs. With this fix, the firewall is able to support up to 64 CVEs per vulnerability rule. If the number of CVEs in the rule is more than 64, the firewall displays a warning when you commit configuration changes.
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-SA-2017-0004).
PAN-64822	Fixed an issue where one or both peers in a high availability (HA) configuration failed to update the time-to-live (TTL) value as expected for synchronized sessions.
PAN-64360	Fixed an issue where the firewall failed to populate the email sender, recipient, and subject information for WildFire reports.
PAN-60591	Fixed an issue where a custom role administrator with commit privileges could not commit configurations using the XML API.
PAN-59204	Fixed an issue where the firewall did not create an IPSec NAT-T session after a tunnel re-key until it originated a tunnel keep-alive. When this issue occurred, the firewall dropped NAT-T packets.
PAN-58516	Fixed an issue on PA-500 and PA-2000 Series firewalls where corruption of an instruction cache caused the firewall to restart. This issue occurred after the firewall was in continuous operation without a restart for hundreds of days.
PAN-56009	Fixed an issue on firewalls installed in an HA active/active configuration where out-of-order jumbo packets caused the dataplane to restart, which resulted in a failover.
PAN-52007	Fixed an issue where QoS statistics for a specific interface were empty after a device reboot.
PAN-48095	Fixed an issue where the Panorama dynamic update schedule ignored the currently installed dynamic update version and installed unnecessary dynamic updates.

PAN-OS 6.1.15 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.15 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



Starting with PAN-OS 6.1.15, all unresolved known issues and any newly addressed issues in these release notes are identified using new issue ID numbers that include a product-specific prefix. Issues addressed in earlier releases and any associated known issue descriptions continue to use their original issue ID.



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
PAN-64917	A security-related fix was made to address CVE-2014-9708 (PAN-SA-2016-0027).
PAN-63073	Security-related fixes were made to prevent denial of service attacks against the web management interface (PAN-SA-2016-0035).
PAN-61468	A security-related fix was made to address CVE-2016-6210 (PAN-SA-2016-0036).
PAN-61104	A security-related fix was made to address a local privilege escalation issue (PAN-SA-2016-0034).
PAN-61046	A security-related fix was made to address a cross-site request forgery issue (PAN-SA-2016-0032).
PAN-58418	Fixed an issue where Panorama could not sync to the NSX manager after a reboot or a failover, which caused a service outage. With this fix, sync works as expected.
PAN-58086	Fixed an issue on firewalls where a process (<i>devsvr</i>) restarted if you committed a configuration that used more than 64 vendor IDs in a single vulnerability protection rule. With this fix, if you commit a configuration with more than 64 vendor IDs in a single rule, you receive a warning that you have exceeded the maximum number of IDs, and the process restart does not occur.
PAN-56650	Fixed an issue where a log collector failed to send the system log to the active Panorama peer in an HA active/passive Panorama configuration after the active peer restarted.
PAN-56280	Fixed an issue where the firewall displayed the status of a 10G SFP+ virtual wire interface as <code>10000/full/up</code> when the configured state of the interface was <code>auto/auto/down</code> . This issue occurred when Link State Pass Through in Network > Virtual Wires was enabled.
PAN-56221	A security-related fix was made to address a cross-site scripting condition in the web interface (PAN-SA-2016-0033).

Issue Identifier	Issue Description
PAN-56200	Fixed an issue where the firewall allowed access to the search engine's cached version of a web page even though the page belonged to a URL category blocked by a policy.
PAN-56034	Fixed an issue where WildFire platforms experienced nonresponsive processes and sudden restarts under certain clients' traffic conditions.
PAN-55560	Fixed an issue on firewalls where a memory condition caused the dataplane to restart with the message <code>Dataplane is down: too many dataplane processes exited</code> .
PAN-55237	A security-related fix was made to address an XPath injection vulnerability in the web interface (PAN-SA-2016-0037).
PAN-54696	Fixed an issue on firewalls where incorrect handling of selective-acknowledgment (SACK) packets caused a decrease in download speeds on SSL-decrypted traffic.
PAN-52379	A security-related fix was made to address CVE-2015-5364 and 2015-5366 (PAN-SA-2016-0025).
PAN-47607	Fixed an issue where the URL field in the URL Filtering log became blank or was logged without a hostname.
PAN-48508	Fixed an issue where the passive Panorama server in an HA configuration did not display application data in the Application Command Center (ACC) or in AppScope.
PAN-47062	Fixed an issue where a VM-Series NSX edition firewall sent Dynamic Address Group information only to the primary virtual system (VSYS1) on the integrated physical firewall at the data center perimeter. With this fix, a VM-Series NSX edition firewall configured to Notify Device Group sends Dynamic Address Group updates to all virtual systems on a physical firewall running PAN-OS 6.1.15 or a later PAN-OS 6.1 release.

PAN-OS 6.1.14 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.14 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
101089	Fixed an issue where a firewall incorrectly applied SSL decryption to traffic in a custom URL category. This issue occurred when the firewall inspected traffic between the client and an explicit HTTP proxy, and the client hello message did not contain server name information (SNI).
100129	Fixed an issue on firewalls in an HA active-passive pair where HA configuration sync failed. This issue occurred when configuration sync from the active firewall happened while the passive firewall was in a state where a local commit failed. With this fix, configuration sync from the active firewall overwrites the configuration on the passive firewall, and configuration sync succeeds.
98684	Fixed an issue on VM-Series firewalls where, if path monitoring for HA used IPv6 addressing, the firewall used the wrong IPv6 address and path monitoring checking failed.
97282	Fixed an issue on PA-7000 Series firewalls where a slot stopped responding due to a memory condition.
96082	Fixed an issue where the firewall responded to Microsoft network load balancing (MS-NLB) multicast packets with the multicast address as the source address.
PAN-57659 95895	A security-related fix was made to address a cross-site scripting (XSS) condition in the web interface (PAN-SA-2016-0031).
95462	Fixed an issue on PA-5000 and PA-7000 Series firewalls where the dataplane repeatedly stopped responding and sessions were logged without an identified application.
95184	Fixed an issue where the GlobalProtect agent failed RADIUS authentication because the firewall did not properly forward the <code>state</code> AVP value to the RADIUS server.
94165	Fixed an issue where the firewall generated WildFire Submissions logs with an incorrect email subject and sender information when sending more than one email to a recipient in a POP3 session.
93770	Fixed an issue where the firewall interpreted a truncated external dynamic list IP address (such as 8.8.8.8/) as 0.0.0.0/0 and blocked all traffic. With this fix, the firewall will ignore incorrectly formatted IP address entries.

Issue Identifier	Issue Description
93392	Fixed an issue where, after you upgraded the firewall to a PAN-OS 6.1 release, a user with a RADIUS administrator user account and a space character in their username could not log on to the CLI.
92621	Fixed an issue where forwarded threat logs used inconsistent formatting between the <code>Request</code> field and the <code>PanOSReferer</code> field. With this fix, the <code>PanOSReferer</code> field uses double quotes for consistency with the <code>Request</code> field.
92523	Fixed an issue where, for firewalls in HA active/active configuration, an Oracle redirect's predict session synchronized to the peer device became stuck in the <code>Opening State</code> because the parent session was not installed on the peer device. With this fix, the firewall ensures the parent session is installed on the peer device and the Oracle redirect's predict session transitions to active state to allow for successful Oracle client-to-server communication.
91269	Fixed an issue where the firewall restarted the dataplane after a process stopped responding.
91034	Fixed an issue on the WildFire platform where, if the <code>snmp.log</code> file was over 5MB, the SNMP daemon (<code>snmpd</code>) process cleared the log file and restarted.
90596	Fixed an issue on PA-5000 Series firewalls where the FPGA did not initialize. With this fix, the FPGA is automatically reprogrammed after an initialization failure so that it can attempt to reinitialize (multiple times) before triggering a boot failure.
89891	Fixed an issue where Threat logs forwarded from the firewall had an extra colon when using TCP for the transport protocol. With this fix, the format of forwarded logs over TCP and UDP is consistent.
87154	Fixed an issue where firewalls stopped forwarding data to the WildFire cloud. With this fix, if the connection to the WildFire cloud fails, the firewall attempts to reconnect after the initial failure and resumes forwarding when successfully reconnected.
86979	Fixed an issue where an incomplete IPSec tunnel configuration (one without an IKE gateway specified) caused the firewall server process to stop responding.
76426	Fixed an issue where VM Series firewalls sent duplicate ICMPv6 echo replies. This issue occurred when neighbors sent IPv6 pings to a firewall virtual interface with a MAC address configured manually in the ESXi server.
67690	Fixed an issue where the firewall reported issues connecting to the BrightCloud URL database.

PAN-OS 6.1.13 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.13 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
98510	Fixed an issue where exported log files did not correctly escape certain characters, such as commas (,), backslashes (\), and equal-to operators (=).
98112	Fixed an issue with firewalls in an HA active/active configuration where session timeouts for some traffic were unexpectedly refreshed after a commit or HA sync attempt.
97763	Fixed an issue where a PA-200 firewall failed to download a PAN-OS software update due to incorrect disk space calculation.
97247	Fixed an issue where a PA-200 firewall failed to download a content update due to disk space issues after a failed AV installation. With this fix, the firewall will, as part of the AV installation process, clean up all temporary files even if AV installation fails.
95622	Security-related fixes were made to address issues identified in the May 3, 2016 OpenSSL security advisory (PAN-SA-2016-0020).
94765	Fixed an issue where NAT translation did not work as expected when the administrator deleted a virtual system (vsys) from a firewall with multiple virtual systems (multi-vsyes) and NAT rules configured without first deleting NAT rules associated with the vsys. With this fix, when the administrator deletes a vsys, the firewall will automatically delete NAT rules associated with that vsys.
94573	Fixed an issue where a firewall dropped incoming PSH+ACK segments from the server.
92610	Fixed an issue on PA-200 firewalls where the firewall stalled during boot-up after an upgrade from PAN-OS 6.1.12 or an earlier PAN-OS 6.1 release to a PAN-OS 7.0 or later release.
PAN-55259 92106	A security-related fix was made to address multiple NTP vulnerabilities (PAN-SA-2016-0019).
PAN-55122 91886	A security-related fix was made to address CVE-2015-7547 (PAN-SA-2016-0021).
91724	Fixed an issue where an autocommit of an incremental antivirus update failed after a reload due to a corrupt virus signatures file and a failed incremental installation. With this fix, incremental content installation has enhanced protections to prevent autocommit failures, and will log additional information to assist with troubleshooting.


Issue Identifier	Issue Description
90842	Fixed an issue where the firewall received an unencrypted empty ISAKMP packet in quick mode that caused a process (<i>ikemgr</i>) to stop responding.
90794	Fixed an issue where a log file (<i>/var/log/wtmp</i>) inflated and consumed the available disk space. With this fix, PAN-OS software uses a log rotation function to prevent log files from consuming more disk space than necessary.
90680	Fixed an issue on PA-500 firewalls where certain processes (<i>l3svc</i> and <i>sslvpn</i>) stopped responding after the firewall attempted a dynamic update.
90553	Fixed an issue where Data Filtering and WildFire Submissions logs for non-NAT sessions contained incorrect or invalid NAT information.
89984	A security-related fix was made to address a stack overflow condition (PAN-SA-2016-0024).
87880	Fixed an issue where the XML API request to test Security policy was not properly targeted to a specified virtual system (<i>vsys</i>), which made the request applicable only to the default <i>vsys</i> . With this fix, the XML API request to test Security policy is able to retrieve results for any previously targeted <i>vsys</i> .
87741	Fixed an issue on PA-3000 Series firewalls where the dataplane restarted after an upgrade.
PAN-52038 86767	A security-related fix was made to address CVE-2015-7547 (PAN-SA-2016-0029).
85531	Additional X-Frame protections introduced in GlobalProtect and SSL VPN pages.
81750	Fixed an issue on PA-200 firewalls where files in the <i>/tmp</i> partition caused a low disk space condition. With this fix, some files in <i>/tmp</i> have been relocated to other partitions to improve disk space allocation.
PAN-48954 81411	Security-related fixes were made to address issues identified in the March 19, 2015 and June 11, 2015 OpenSSL security advisories (PAN-SA-2016-0028).
81333	Fixed an issue where managed firewalls and appliances were unable to connect to Panorama using the master key after a factory reset (or RMA).
79463	Fixed an issue where CPU memory on a PA-7050 firewall spiked when attempting to view reports in the Application Command Center (ACC). This issue occurred when task creation notifications were not processed properly and, as a result, the Log Collector did not terminate failed requests as expected. With this fix, task creation notifications are processed appropriately and failed tasks are properly terminated.
73266	Fixed an issue on PA-200 firewalls where, if an upgrade failed because the firewall did not have sufficient disk space to install a base image and a delta image, you could not work around the problem by deleting the installation image in the revertible partition to reclaim disk space. With this fix, if you require additional disk space for installation, you can delete the installation image from the revertible partition (Device > Software).

PAN-OS 6.1.12 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.12 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
93612	A security-related fix was made to address a privilege escalation issue.
93072	A security-related change was made to address an issue in the policy configuration dialog.
PAN-55477 92481	A security-related fix was made to address CVE-2016-0800 (DROWN), CVE-2016-0703, and CVE-2016-0704 (PAN-SA-2016-0030).
92413	A security-related change was made to address a boundary check that caused a service disruption of the captive portal.
92391	Fixed an issue where firewall Traffic logs displayed unusually large byte counts for sessions passing through proxy servers.
92293	A security-related fix was made to address CVE-2016-1712.
91685	Fixed an issue where an M-100 appliance in Log Collector mode disconnected when the management server process (<i>mgmtsvr</i>) restarted.
90256	Fixed an issue where decrypted SSH sessions were not mirrored to the decrypt mirror interface as expected.
90194	Fixed an issue where firewalls without any WildFire public signatures (had never downloaded any or old signatures had been deleted) did not properly leverage WildFire private cloud signatures when monitoring traffic.
89743	Fixed an issue where commits failed due to processes (<i>configd</i> and <i>mgmtsvr</i>) that stopped responding. This issue was caused by memory corruption related to the WildFire deployment schedule.
89588	Fixed an issue where packets that had to be retransmitted during SSL decryption were not handled correctly, which resulted in a depleted software packet buffer.
89503	Fixed an issue where user-group mappings were not properly populated into the dataplane after a firewall reboot.
89385	Fixed an issue with firewalls in an HA active/active configuration where session timeouts for some traffic were unexpectedly refreshed after a commit or HA sync attempt.  This fix introduced a known issue: 97806 .

Issue Identifier	Issue Description
88696	Fixed an issue where, under certain conditions, a process (<i>mpreplay</i>) frequently restarted due to excessive internal messaging.
88157	Fixed an issue with reduced throughput for traffic originating on the firewall and traversing a VPN tunnel.
87833	Fixed an issue where WildFire updates caused the interface to flap.
86970	Fixed an issue where decryption on the firewall did not function when using Chrome to browse certain websites because Chrome eliminated insecure fallback to TLS 1.0.
86916	Fixed an issue where traffic bursts entering a PA-3000 Series firewall caused short-term packet loss even though the overall dataplane utilization remained low. This issue was typically observed when two firewall interfaces on the same firewall were connected to each other. With this fix, internal thresholds were modified to prevent packet loss in these conditions.
86686	Security-related fixes were made to address issues reported in the October 2015 NTP-4.2.8p4 Security Vulnerability Announcement .
86251	Fixed an issue where an administrator was unable to retrieve log partition utilization using SNMP after adding additional virtual disk space on Panorama.
86122	Fixed an issue where an LACP Aggregate Ethernet (AE) interface using SFP copper ports remained down after a dataplane restart.
83361	Fixed an issue where the DoS classification counter stopped at an abnormally high value. This caused flood type false positives in the Threat logs, causing the firewall to appear as if it reached maximum session capacity.
83337	Fixed an issue where firewalls generated multiple core dumps after a reboot when incoming packets were forwarded to the dataplane while an autocommit was still processing. With this fix, packets are not forwarded to the dataplane until an in-process autocommit is complete.
79729	Fixed an issue with firewalls in an HA configuration where a commit operation aborted for all daemons and then the DHCP daemon stopped responding. This occurred when the <code>set deviceconfig high-availability group {group-name} configuration-synchronization enabled option</code> was set to <code>no</code> .
78742	Fixed an issue where single direction RST/FIN SSL proxy flows did not transition as expected from an in-process TCP session timer to the timer used for closed sessions, which resulted in proxy session exhaustion during periods of high traffic (identified by a global counter error: <code>proxy_flow_alloc_failure</code>).
77460	Fixed an issue on a firewall with an expired BrightCloud license where the specified vendor was unexpectedly and automatically changed from BrightCloud to PAN-DB when any feature auth code was pushed from Panorama to the firewall.

PAN-OS 6.1.11 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.11 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
93228	Fixed an issue on PA-7050 firewalls in an HA active/active configuration where jumbo frames that included the DF (do not fragment) bit were dropped when crossing dedicated HA3 ports.
91934	Fixed an issue that occurred after upgrading to PAN-OS 6.1.8, 6.1.9, or 6.1.10 releases where the firewall silently failed to download WildFire private cloud signature updates and then reported errors when trying to install the updates.
91771	Fixed an issue where a firewall did not send TCP packets out during the transmit stage in the same order as those packets were received.
91227	Fixed an issue where a process (<i>pan_comm</i>) stopped responding during a certificate dump of expired certificates.
90752	Fixed an issue on firewalls set to FIPS mode where importing a CSR signed certificate with a private key failed due to a certificate decryption failure.
89317	Fixed an issue where improper data pattern ordering occurred after an administrator deleted data patterns from an existing Data Filtering profile, which subsequently caused an error (<i>rule is already in use</i>) when attempting to add a new data pattern. With this fix, you can add or delete data patterns in any order.
88570	Fixed an issue where a Neighbor Solicitation (NS) packet—used to refresh IPv6 neighbor tables—was sent out through a VLAN interface without a VLAN tag. The NS packet was tagged correctly when the neighbor entry was initially created but the packet used to refresh the table was sent without the tag, which caused the table update to fail when the neighbor did not receive an appropriately tagged response.
88191	A security-related fix was made to address information leakage in systems log that impacted the web interface.
87158	Fixed an issue where some packets were duplicated in the egress stage. This occurred on multi-dataplane firewalls when traffic traversed from virtual system to virtual system or from virtual system to a shared gateway. An update has been made to prevent packet duplication.
86723	Fixed an issue where a dataplane restarted when client-to-server traffic exceeded 4GB and included HTTP GET or POST requests that had the source IP address in the Origin header.

Issue Identifier	Issue Description
85878	In response to an issue where DNS queries sometimes caused a Log Collector to run too slowly and caused delays in log processing, the <code>debug management-server report-namelookup disable</code> CLI command is added to disable DNS lookups for reporting purposes.
85358	Fixed an issue where SSL decryption sessions were not cleared after executing the <code>clear session all filter ssl-decrypt yes</code> CLI command (or any other session clearing command that used the <code>ssl-decrypt yes</code> filter). With this fix, SSL decrypt sessions are cleared as expected when executing session clearing commands that include the <code>ssl-decrypt yes</code> filter.
84239	Fixed an issue where a read-only superuser was able to perform a commit when using XML API (but not via the web interface). With this fix, read-only superusers cannot use XML API to perform commits.
82756	Fixed an issue where custom reports were not sent out by the Email Scheduler.
82087	Fixed an issue where a firewall displayed an alert for low disk space. With this fix, the <code>/opt/content</code> directory was removed to improve the disk cleanup process.
81868	Fixed an issue with a packet buffer (FPTCP) leak and resolved a few dataplane-to-management plane connection issues, as well.
81408	Fixed an issue where shared address objects that are not used in Security policy rules were pushed to firewalls even when Panorama Settings (Panorama > Setup > Management) was configured to not Share Unused Address and Service Objects with Devices .
80507	Fixed an issue in Panorama where Threat and Content names for certain threats did not appear in ACC reports, predefined reports, and spyware reports. This issue occurred only on PA-7000 Series firewalls managed by Panorama and only during an Antivirus update.
78317	Fixed an issue where the management plane in an HA active/passive configuration restarted due to a dataplane process (<code>mprelay</code>) that stopped responding when it experienced memory corruption and encountered unexpected behavior from the FIB pointer.
74944	Fixed an issue where SSL traffic caused a service disruption.
74443	A security-related fix was made to address CVE-2015-0235.
73082	Fixed an issue where a firewall process (<code>all_pktproc</code>) stopped responding due to an issue with NAT pool allocation.

PAN-OS 6.1.10 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.10 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
91110	Fixed an issue on firewalls running PAN-OS 6.1.9 where autocommit failed after performing a factory or private data reset.
89752	A security-related fix was made to address a buffer overflow condition.
89750	A security-related fix was made to address a stack underflow condition.
89745	Fixed an issue where some URLs were categorized incorrectly as <code>Not-Resolved</code> when categorization required a cloud inquiry. This occurred when a category for the URL did not exist, yet, in the dataplane or management plane cache.
89717	A security-related fix was made to ensure the appropriate response to special requests received through the API interface.
89706	A security-related fix was made to prevent some CLI commands from improperly executing code.
88439	Fixed an issue on a PA-3000 Series firewall where a dataplane constantly restarted due to a hardware content matching memory issue.
87422	Fixed an issue where multicast traffic was dropped when the source started sending group traffic because there was no corresponding multicast route or FIB entry on the firewall. With this fix, the multicast route is updated more quickly and packets are enqueued instead of dropped while the firewall waits for the updated route information.
86947	Fixed a rare issue where an active firewall in a high availability (HA) configuration incorrectly synced to the configuration from the passive firewall when a second commit was performed on the active firewall before a previous commit was completed.
86365	Fixed an issue where decryption policy profile references caused commit failures.
86321	Fixed an issue where SSH decryption caused a dataplane memory leak and restart.
84678	Fixed an issue with the way the management plane performed updates through HTTP and HTTPS calls, such as for block list and content updates.
84595	Fixed an issue with HTTP requests generated by the firewall when retrieving custom Dynamic Block Lists.

Issue Identifier	Issue Description
84339	Fixed an issue where a single session consumed the majority of the packet buffer resources. With this fix, you can use information in the output of the <code>show running resource-monitor ingress-backlogs</code> command to Identify Sessions That Use an Excessive Percentage of the Packet Buffer and then use the <code>request session-discard</code> CLI operational command to manually discard sessions as needed.
82470	Fixed an issue with IPsec tunnel throughput performance caused by incorrect hardware tagging.
81743	Fixed an issue where URL categorization failed for some URLs due to an issue with message buffer size.
80567	In response to an issue where race conditions affecting Block IP table operations inadvertently caused some packets to be marked as <code>drop ip block</code> without any entry in the Block IP table.
79493	Fixed an issue where the routing process (<i>routed</i>) stopped responding when the firewall was configured to use an Open Shortest Path First (OSPF) Not-So-Stubby Area (NSSA).
74333	Fixed an issue where incremental updates for new and updated registered IP addresses were failing when registration events were occurring through the XML API. With this fix, integrating the updates for registered IP addresses no longer fails when using the XML API (on either standalone firewalls and appliances or those in high availability (HA) configurations).
70419	Fixed an issue where an M-100 appliance ran out of memory and shutdown when running multiple python & ipmitool processes.
67173	Fixed an issue where, if a user pushed a certificate authority (CA) to the firewall through templates, the firewall could not use the CA to sign certificates generated on the firewall.

PAN-OS 6.1.9 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.9 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
88869	Fixed a performance degradation issue on a VM-Series firewall with eight cores when threat scanning was enabled when attempting to process large transaction-specific SSL traffic types. Additionally, this fix addressed an intermittent issue where the GlobalProtect MSI file failed to download after a user authenticated to the portal page.
88382	Fixed an issue in a high availability (HA) active/active configuration with unexpectedly short (20 second) timeouts that occurred when an HA2 session sync message failed. This issue was due to an ARP problem between dataplanes in the HA configuration when the HA2-backup was in use and using either IP or UDP transport mode. With this fix, unexpectedly short session timeouts no longer occur due to this issue.
86938	The client certificate used by PAN-OS and Panorama to authenticate to the PAN-DB cloud service, the WildFire cloud service, and the WF-500 appliance expired on January 21, 2016. The expiration results in an outage of these services. To avoid an outage, either upgrade to content release version 550 (or a later version) or upgrade PAN-OS and Panorama instances running a PAN-OS or Panorama 6.1 release to PAN-OS (or Panorama) 6.1.9 or a later release.
86390	Fixed an issue where a virtual system (vsys) created in a Panorama template did not display where expected when the first two characters of the vsys name was "sg" (such as <code>sg01</code>). With this fix, Panorama no longer allows you to create a vsys with a name that begins with "sg" in a Panorama template.
86193	Fixed an issue in a high availability (HA) configuration where LDAP group mappings did not properly refresh after a firewall became the active peer again after going through the passive state. This was due to a variable that was not initialized properly and was then used in an error case. With this fix, LDAP variables are properly initialized to avoid this LDAP group mapping issue.
86075	Fixed an issue on a PA-3060 firewall where the size of the SML VM <i>EmlInfo</i> software pool was less than expected. With this fix, the size of the SML VM <i>EmlInfo</i> software pool is increased to the expected value.
85863	Fixed an issue where multicast traffic sent over a virtual wire (vwire) with Multicast Firewalling disabled (Network > Virtual Wires > <vwire>) caused high CPU and packet buffer depletion.

Issue Identifier	Issue Description
85801	Fixed an issue where a firewall that was forwarding logs to multiple Panorama management servers and Log Collectors stopped forwarding logs to any appliance after an administrator suspended log forwarding on the active primary Panorama server. With this fix, the firewall continues to forward logs to all Panorama management servers and Log Collectors except any appliance for which an administrator specifically suspends log forwarding.
85383	Fixed an issue where the native Android VPN client failed to connect to GlobalProtect when using certificate-based authentication.
85285	Fixed an issue where output from the <code>show ntp</code> command did not always display the correct NTP status. Primarily, this issue occurred when there was only one NTP server configured and, even when correctly connected to the NTP server, the output of the <code>show ntp status</code> command displayed as <code>rejected</code> . With this fix, output from the <code>show ntp</code> command correctly displays NTP status as <code>synchronized</code> after the firewall successfully connects to an NTP server.
85099	Fixed an issue in a high availability (HA) configuration where a process (<code>mprelay</code>) on the passive device stopped responding after an upgrade from a PAN-OS 6.0 release. This issue was due to a change to HA messages in PAN-OS 6.1 releases for LSVPN traffic that conflicted with the peer firewall that was still running a PAN-OS 6.0 release. With this fix, the firewall ignores the conflicting information in the HA message during that period in the upgrade process when the two firewalls in an HA configuration are running different PAN-OS releases.
84851	Fixed an issue where the virtual system (vsys) ID on the firewall was computed incorrectly when Panorama pushed a template with Force template value enabled and containing virtual system information to the firewall.
84496	Fixed an issue on PA-7000 Series firewalls where excessive or prolonged log queries caused a memory leak on the Log Processing Card (LPC).
84494	Fixed an issue where the session end reason for a single threat ID was reported differently depending on which decoder was used. With this fix, only one session end reason (<code>threat</code>) is reported for all blocked SMTP traffic regardless which decoder is used.
84465	Fixed an issue where the external interface on an LSVPN satellite was unable to establish an LSVPN connection to the active-primary firewall in an HA active/active configuration that was acting as the GlobalProtect portal or gateway when the external interface of the satellite was configured as a DHCP client. (This failure occurred even though an LSVPN connection was successfully established with the active-secondary firewall.) With this fix, the LSVPN satellite (with the external interface configured as a DHCP client) successfully establishes an LSVPN connection to both firewalls (active-primary and active-secondary) after a reboot.
84008	Fixed an issue where an LSVPN IPsec tunnel went down when the hard key lifetime expired during a re-key. With this fix, the soft key lifetime is adjusted so that the hard key lifetime does not expire before the re-key finishes.
83902	Fixed an issue where monitoring an SNMP OID (.1.3.6.1.2.1.25.2.3.1.5.41) for disk space resulted in incorrect values on volumes over 2TB in size.
83657	Fixed an issue where Panorama did not properly push device or template configurations for NTP, send-hostname-in-syslog, or WildFire settings to a device.
83454	Fixed an issue with IPv6 traffic that had an extension header and caused jitter when passing through a PA-7000 Series firewall in a high availability (HA) active/active configuration.

Issue Identifier	Issue Description
83145	Fixed an issue on a PA-7050 firewall where an interface in tap mode unexpectedly transmitted traffic that was received on that interface.
83140	Fixed an issue where packet processing on a VM-Series firewall caused the firewall to stop forwarding traffic.
82916	Fixed an issue where the trusted CA store on the firewall was missing the QuoVadis root CA2 and root CA3 G3 certificates. With this fix, both these QuoVadis certificates are included in the trusted CA list.
82913	Fixed an issue where ToS headers were not set correctly in Encapsulating Security Payload (ESP) packets across VPN tunnels.
82838	Fixed an issue where the User-ID process (<i>userid</i>) stopped responding when reading config messages from the Terminal Services (TS) agent.
82605	Fixed an issue where policy-based forwarding (PBF) with Enforce Symmetric Return enabled (Policies > Policy Based Forwarding > <pbf-rule> > Forwarding) caused offloaded PBF sessions to fail when attempting to egress the firewall.
82118	Fixed an issue in QoS Statistics (Network > QoS) where data was displayed only on the Bandwidth tab; all other tabs (Applications, Source Users, Destination Users, Security Rules, and QoS Rules) were empty.
81812	Fixed an issue where a firewall did not accurately check certificate revocation status via OCSP because the OCSP request did not include the HOST header option. With this fix, the firewall uses the HOST header option as expected and successfully retrieves the revocation status of the certificate in response to OCSP requests.
81522	Fixed an issue where a firewall allowed commits to succeed even when there were no superuser administrator accounts included in the configuration. This would cause the firewall to be inaccessible. With this fix, a commit succeeds only if there is at least one local superuser account in the configuration; if none exist, the commit fails.
80766	Fixed an issue where dataplane 0 (DPO) on the passive firewall in a high availability (HA) configuration restarted after a session was established on the active firewall interface when that same interface did not also exist on the passive firewall.
80631	Fixed an issue in a high availability (HA) configuration where the ports on the passive firewall did not come up when the passive link state in Active/Passive Settings was set to auto (Device > High Availability > General) .
78848	Fixed a rare issue where a commit (such as an antivirus update or FQDN refresh) caused the firewall to stop processing traffic. This issue occurred after a high availability (HA) synchronization event when the autocommit triggered by the synchronization event was ignored. With this fix, a force commit request is automatically and repeatedly generated until successful.
78214	Fixed an issue where attempts to regenerate metadata caused a process (<i>update_vld_itvl_idx</i>) to stop responding when encountering a corrupt log file (a log file that contained invalid data). With this fix, the metadata regeneration process skips log files that contain invalid data so that regeneration task is successfully completed.
77236	Fixed an issue where importing a certificate more than once with different names caused the dataplane to stop responding when the certificate was used for SSL Inbound inspection.

Issue Identifier	Issue Description
76197	Fixed an issue where firewall Traffic logs displayed unusually large byte counts for http-proxy and http-video counters due to frequent application shifts between those application-type packets within a single proxy session.
74654	Fixed an issue on an M-100 device where an attempt to download content release versions failed due to a lack of disk space. This issue occurred when continuous XML API queries filled the /opt/pancfg partition because <code>stop</code> messages were getting dropped between Panorama and the Log Collector and queries were not properly removed when no longer needed. With this fix, <code>stop</code> messages should not be dropped. Additionally, in case <code>stop</code> messages are dropped for any other reason, a timeout setting for queries is in place to ensure that stale queries are removed from disk space before causing a storage space issue.
68353	Fixed an issue where a process (<i>routed</i>) stopped responding when BGP received a redistributed route from OSPF that was also the BGP aggregate route.
66285	Fixed an issue where the web interface certificate did not properly sync between HA peers, which led to a race condition that caused a commit request to fail.

PAN-OS 6.1.8 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.8 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
87280	Fixed an issue where the number of SSL free memory chunks was depleted to 0, which caused a disruption in SSL decryption-related traffic.
85721	Fixed an issue where firewalls with a specific OCZ Deneva hard disk (model DENCSTE251M21) configured in a RAID and running PAN-OS 6.1.2 or later releases experienced RAID errors.
85091	Fixed an issue on a firewall where software packet buffers were being depleted. With this fix, the firewall will dynamically adjust the TCP receive window based on peer traffic to avoid software packet buffer depletion. Additionally, there is a fix for a memory leak in error handling of SSL forward proxy mode and the size of the software buffer pools is increased.
85065	Fixed a CLI input parsing issue that caused a process on the management plane to stop responding when processing unexpected input.
84495	Fixed an issue where, in some cases, generating output for the <code>show running url-cache all</code> CLI command caused a short delay in communication with the dataplane. With this fix, to avoid this communication delay, the output of the <code>show running url-cache all</code> command is no longer included when generating the tech support file.
84167	Fixed an issue where a firewall incorrectly reordered certain TCP traffic during transmit stage.
84046	Fixed an issue where SSL decryption failed when a certificate was rejected due to a missing or empty <code>basicConstraints</code> extension. With this fix, an exception is added to allow a missing or empty <code>basicConstraints</code> extension for self-signed non-CA certificates, and the following behaviors will be applied to CAs with regard to <code>basicConstraints</code> extensions: <ul style="list-style-type: none">• If the CA has an extension <code>basicConstraints=CA:TRUE</code>, then allow the CA.• If the CA has an extension <code>basicConstraints=CA:FALSE</code>, then block the CA, but allow device-trusted CAs, including default CAs and imported CAs.• If the CA has does not have a <code>basicConstraints</code> extension, then block the CA, but allow device-trusted CAs, including default CAs and imported CAs, and allow self-signed CAs.
83907	Fixed an issue where the <code>debug dataplane packet-diag set log counter <counter-name></code> CLI command did not accept counter names longer than 31 characters, which prevented administrators from enabling (or disabling) such counters in system logs.

Issue Identifier	Issue Description
83889	Fixed an issue where a PA-7050 firewall incorrectly dropped non-TCP and non-UDP fragmented traffic, such as EtherIP traffic.
83844	Fixed an issue where a memory leak caused a PA-200 firewall to reboot.
83592	Fixed an issue where the User-ID process (<i>userid</i>) went into a reboot loop and caused the passive firewall in a high availability (HA) configuration to restart. This was due to bulk and incremental updates of terminal services users.
83519	A security-related fix was made to address CVE-2015-5600.
83293	Fixed an issue in Panorama where SNMPv3 settings were removed and could not be updated when modifying an existing SNMPv3 device template.
83253	Fixed an issue where video calls failed when H.245 (<i>openlogicalchannelack</i>) packets referenced a pre-NAT address.
83001	In addition to the fix delivered in PAN-OS 6.1.7 (where old logs were incorrectly purged when the available disk space on an M-100 was reported as 0 bytes during an upgrade), Panorama 6.1.8 and later releases on an M-100 with zero disk space display an error when attempting to commit to Collector Group (<code>Failed to commit collector config</code>) or a warning when attempting to commit to Panorama (<code>Disk <disk-ID> on log collector <log-collector-id> in group <group-ID> has a size of zero bytes</code>).
82927	Fixed an issue where a firewall used an incorrect MAC address as the source MAC address for HA2 traffic when HA2 keep-alive messages were enabled and HA2 transport mode was set to IP or UDP. With this fix, the firewall uses the MAC address specified on the interface for HA2 keep-alive messages regardless of the specified HA2 transport mode.
82849	Fixed an issue on a Panorama virtual appliance using a Network File System (NFS) storage partition where the file system integrity check incorrectly failed for the NFS directory, which caused the NFS mount to fail when rebooting Panorama after an upgrade to Panorama 7.0.
82621	Fixed an intermittent issue on a PA-7050 firewall where traffic was dropped when the log interface and dataplane interfaces were both configured on the same Network Processing Card (NPC).
82377	Fixed an issue where, in a Large Scale VPN (LSVPN) configuration, a GlobalProtect gateway incorrectly installed the previously allocated IP address for the GlobalProtect satellite as the next hop for the routes advertised by satellites. With this fix, the GlobalProtect gateway removes any old IP addresses allocated to the satellite and correctly installs the new IP address allocated to the satellite as the next hop for the routes advertised by satellites.
82326	Fixed an issue where additional locked users are not displayed when you click More in the web interface (Devices > Authentication-Sequence > Locked Users).
82136	Fixed an issue where packets that matched a policy-based forwarding (PBF) rule with Action set to No PBF (Policies > Policy Based Forwarding > <pbf-rule> > Forwarding) were dropped when offloading was enabled. With this fix, offloaded sessions are passed as expected even when the traffic matches a PBF rule with Forwarding set to No PBF .
82095	Fixed an issue where a commit request did not finish processing due to a process (<i>routed</i>) that stopped responding.

Issue Identifier	Issue Description
81944	Fixed an issue where patch management for a GlobalProtect host information profile (HIP) failed to identify missing patches when the Check setting for patch management in HIP Objects criteria was set to has-all , has-any , or has-none (Objects > GlobalProtect > HIP Objects > Patch Management > Criteria).
81927	Fixed an issue where a firewall stopped submitting files to a WildFire cloud (public or private) when a CPU process (<i>varrcvr</i>) stopped responding. This issue occurred when receiving an email with a subject line containing more than 252 characters.
81830	Fixed an issue where SSL Forward Proxy did not include the appropriate TLS 1.2 extension (<i>Signature Algorithms</i>) in Client Hello messages, which prevented successful interoperability with some Microsoft websites.
81581	Fixed an issue where a process (<i>userid</i>) was unable to accommodate a large number of HIP reports during HA synchronization, which caused abnormally high CPU and memory utilization on the firewall.
81415	Fixed an issue on PA-7000 Series, PA-5000 Series, PA-3000 Series, and PA-500 firewalls where an Aggregate Ethernet (AE) interface was unable to transmit an ARP request on a tagged subinterface to the neighboring device.
81370	Fixed an issue where the firewall was unable to allocate a large memory block, which caused sessions to fail. This fix ensures adequate resources are available for a large memory block when needed.
81367	A security-related fix was made to address CVE-2015-4024.
81301	Fixed an issue on a firewall with decryption enabled where insufficient buffer space resulted in discarded SSL sessions.
81241	Fixed a rare issue where NAT traffic was dropped after a failed commit attempt.
80753	Fixed an issue on a PA-3060 firewall where a network outage occurred when the number of active sessions reached 100,000. With this fix, the maximum number of detector threats (<i>dthreats</i>) is increased to avoid this issue.
80702	Fixed an issue in a high availability (HA) configuration where the ARP table synced with the primary peer but was refreshed only on dataplane 0 (DP0) of the passive peer, which caused ARP entries to expire prematurely on the passive firewall when their TTL reached 0.
80687	Fixed an issue on PA-7050, PA-5000 Series, and PA-3000 Series firewalls where software packet buffers were depleted (although eventually recovered) when receiving TCP packets with large payloads. With this fix, modifications to processes for allocating software buffers and handling TCP congestion ensure that software packet buffers do not get depleted due to packets with large payloads.
80648	Fixed an issue where a device group commit failed when using the destination interface in a NAT rule configured on Panorama.
80389	Fixed an issue on a PA-5060 firewall where internal packet path monitoring failed when under a heavy load. With this fix, internal packet path monitoring is forwarded using a priority setting that prevents these failures even when experiencing high traffic conditions.
80064	Fixed an issue where a process (<i>reportd</i>) stopped responding during the shutdown sequence in Panorama due to a memory access violation.
79746	Fixed an issue on a PA-2000 Series firewall where an Aggregate Ethernet (AE) interface was unable to transmit an ARP request on a tagged subinterface to the neighboring device.

Issue Identifier	Issue Description
78624	Fixed an issue where the active-secondary firewall in an HA active/active configuration was incorrectly responding to ARP requests for the IP address used in the destination NAT rule with binding to the active-primary firewall.
78568	Fixed an issue where PA-7050, PA-5000 Series, and PA-3000 Series firewalls experienced a memory leak associated with improper purging of old, replaced entries in the ARP/ND table when the table reached capacity.
78426	Fixed an issue where a CPU process (<i>pan_dhcpd</i>) spiked when DHCP NAK packets were received on the DHCP relay interface.
78210	Fixed an issue in a high availability (HA) active/passive configuration where the multicast tree failed to converge non-offloaded multicast traffic as quickly as expected after a failover. With this fix, the multicast tree convergence time is reduced for non-offloaded multicast traffic after an HA active/passive failover.
78040	Fixed an issue where the output of the <code>show zone-protection zone</code> CLI command did not correctly display zone protection information for a defined virtual system (VSYS).
77376	Fixed an issue where a gateway Config refresh on a satellite device (Network > IPsec Tunnels > Gateway Info (for a gateway) > <code><gateway></code> > Refresh GW Config) caused a delay in tunnel installation and resulted in connectivity issues for the duration of the delay.
77330	Fixed an issue where unsupported ciphers were not added to the SSL decryption exclude list as expected.
76981	Fixed an issue where a certificate containing a space character (" ") in the Common Name field of the certificate prevented the firewall from establishing a secure syslog connection with the syslog server. With this fix, firewalls establish syslog connections as expected even when a certificate contain space characters in the Common Name.
76481	Fixed an intermittent issue where a Category for a session in the URL Filtering log did not match the actual categorization of that session. With this fix, the logic for removing expired or unresolved URL cache entries is improved so that a Category in the URL Filtering log stays in sync with the actual categorization of a session.
73146	Fixed an issue where the IKE process (<i>iked</i>) restarted and caused IPsec VPN tunnels to go down.
70719	In response to an issue where a dataplane restarted due to an incorrect flow ID, PAN-OS 6.1.4 and later releases included additional checks to help prevent the dataplane from restarting due to this issue. With this fix in PAN-OS 6.1.8, those PAN-OS 6.1.4 modifications are further modified to provide a more complete solution that avoids inadvertently dropping traffic (both IPv4 and IPv6) affected by this issue.
65972	Fixed an intermittent issue where, after a failover in a high availability (HA) active/passive configuration, OSPF adjacencies on the new active peer were not properly formed, which caused both neighbors to claim the role of Designated Router (DR), which also means neither becomes the Backup Designated Router (BDR). With this fix, the adjacencies form as expected and the DR and BDR elections are correctly negotiated.

PAN-OS 6.1.7 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.7 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



In an HA configuration, a peer running PAN-OS 6.1.7 or a later release will not synchronize properly with a peer running PAN-OS 6.1.6 or an earlier release, which causes dropped packets if a failover should occur while HA peers are running in such a configuration. To avoid this issue, upgrade both HA peers as close together as possible if peers are running PAN-OS 6.1.6 or an earlier release.

Issue Identifier	Issue Description
84094	Fixed an issue where the User Activity Report (Monitor > PDF Reports) contained no statistics for users with a domain+username string-length that exceeded 32 characters.
83155	Fixed an intermittent issue that caused display problems for Traffic and Threat logs in the Panorama™ web and command line interfaces.
83001	Fixed an issue on an M-100 appliance where available disk size was reported as 0 bytes during an upgrade. This incorrectly caused old logs to be purged from the other Log Collectors in the group in an attempt to adhere to the configured log quota for the group.
82724	Fixed an issue where old registered IP addresses in a Dynamic Address Group on a high availability (HA) active/passive pair were deleted from the passive firewall when that firewall switched from non-functional to passive state and received an incremental update of registered IP addresses from the active firewall. This fix also addressed a related issue in an HA active/active configuration where the active-secondary firewall retained old IP addresses in the Dynamic Address Group after switching to a functional state when the active-secondary firewall switched to non-functional state and all IP addresses in the Dynamic Address Group became unregistered on the active-primary firewall.
82717	Fixed an issue where a dataplane stopped responding after a reboot due to an initialization issue on SFP+ ports.
82563	Fixed an issue in Panorama 6.1.5 and Panorama 6.1.6 where multiple erroneous error messages were triggered when running the <code>scp export config-bundle to <username@host:path></code> command. Although this issue was cosmetic (the displayed errors were not real), with this fix, these error messages are no longer triggered erroneously.
82370	Fixed an intermittent issue where a dataplane process (<i>mprelay</i>) experienced a memory leak that caused the virtual memory to increase until it triggered a dataplane restart.
82310	In response to a fragmentation issue, virus patterns are split into smaller chunks to reduce the possibility of memory allocation failure.
81955	Fixed an issue on a firewall where files were not sent to WildFire™ as expected when the first 8 bytes of the file were split across different packets or decrypted buffers.
81816	Removed support for SSLv3 on Panorama for connections to managed devices.
81797	Fixed an issue where ASCII and special characters were not supported in the user activity report username field.

Issue Identifier	Issue Description
81584	Fixed an issue in Panorama 6.1.3 and later releases where output from the <code>show ntp</code> command did not always display the correct NTP status. Primarily, this issue occurred when there was only one NTP server configured and, even when correctly connected to the NTP server, the <code>show ntp status</code> displayed as <code>rejected</code> . With this fix, output from the <code>show ntp</code> command correctly displays NTP status as <code>synchronized</code> .
81577	Fixed an issue where custom URL categories associated with a Decryption policy did not match traffic destined for a proxy server.
81572	Fixed an issue on a PA-7000 Series firewall that displayed incorrect timestamps in Traffic, Threat, and URL Filtering logs.
81535	Fixed an issue where the group list was empty after pushing the group mapping configuration from Panorama to a multi-vsyt firewall during an attempt to configure users in a Security policy rule even though the group mapping state was synchronized.
81452	Fixed an issue where switching context from the Panorama web interface to a managed firewall did not indicate whether the administrator was logged in over an encrypted SSL connection; the System log message was always <code>User admin logged in via Panorama from x.x.x.x using http</code> regardless whether the connection was encrypted. With this fix, the System log now specifically reports <code>User admin logged in via Panorama from x.x.x.x using http over an SSL connection</code> when the administrator is connected through an encrypted SSL connection to differentiate from non-encrypted connections.
81219	Fixed an issue with stability when adding Log Collectors to a Collector Group.
81115	Fixed an issue where administrators experienced long delays when executing log queries consisting of multiple attributes.
81110	Fixed a session reuse issue where an incoming SYN/ACK packet for an established session caused a failure in TCP reassembly, which resulted in a dropped packet even the Reject Non-SYN TCP option was disabled (Network > Network Profiles > Zone Protection > <Zone Protection profile> > Packet Based Attack Protection > TCP Drop). With this fix, initiating session reuse with a SYN/ACK packet is successful regardless of the Reject Non-SYN TCP setting.
81058	Fixed an issue on PA-7000 Series firewalls where NAT Dynamic IP fallback did not correctly translate resources, which resulted in dropped packets.
80933	Fixed a rare issue where a PA-7000 Series firewall experienced heartbeat failures on the HA1 and HA1 backup links that caused split brain in a high availability (HA) configuration.
80840	Fixed an issue where the URL filter did not correctly parse the common name (CN) value when a MAC address was specified as the CN value in the server certificate.
80789	Fixed an issue with an M-100 appliance where logs on log collectors were not removed from the queue as expected. With this fix, logs are removed from the queue as expected without the need to restart the management server.
80720	Fixed an issue where a firewall in a high availability (HA) configuration experienced a dataplane restart when the packet processing daemon terminated due to a double free condition associated with a specific packet buffer (<code>fptcp</code>).
80669	Fixed an issue on firewalls running in CC mode where the management server would restart when the firewall attempted to send an SNMPv3 trap.

Issue Identifier	Issue Description
80624	Fixed an issue where administrators experienced delays accessing the firewall web interface when the firewall reconnected to Panorama and had a large number of logs to send.
80532	Fixed an issue where files were not being forwarded as expected to the WildFire cloud (public or private) due to a terminated process (<i>varrcvr</i>). This issue occurred when the Subject field in forwarded emails contained non-ASCII characters.
80386	Fixed an issue where a configuration override failed when pushing system log settings to firewalls from Panorama resulting in the following error: <code>edit failed, may need to override template object informational first.</code>
80251	Fixed an issue on a firewall with X-Forwarded-For (XFF) enabled where a dataplane restarted with multiple core files (<i>all_pktproc</i> , <i>flow_ctrl</i> , and <i>flow_mgmt</i>) when the firewall received percent-encoded HTTP requests from a proxy server.
79960	Fixed an issue where the firewall sent an extra carriage return line feed (CRLF) in HTTP/1.1 POST packets when requesting an update from the BrightCloud URL database. This issue occurred when using a proxy server, which correctly rejects the packets and returns HTTP/1.1 400 Bad Request messages due to the extra CRLF (per RFC 7230).
79925	Fixed an issue where virtual wire (<i>vwire</i>) path monitoring failed and the firewall stopped sending ICMP packets over the <i>vwire</i> interface after a high availability (HA) failover.
79893	Fixed an intermittent issue where a process (<i>routed</i>) stopped responding on a firewall in a high availability (HA) configuration when that firewall was suspended using the <code>request high-availability state suspend</code> command and subsequently made functional using the <code>request high-availability state functional</code> command. With this fix, performing these commands successively on either firewall in an HA configuration no longer causes the <i>routed</i> process on the firewall to stop responding.
79854	Fixed an issue where Panorama was unable to display System and Config logs for PA-7050 firewalls.
79719	Fixed a rare issue where a dataplane restarted when multiple processes (<i>flow_ctrl</i> and <i>mprelay</i>) stopped responding due to a software buffer leak.
79535	Fixed an issue in a high availability (HA) configuration where the monitored destination IP address for Path Monitoring displayed as <code>up</code> even when unavailable, preventing the firewall from displaying as <code>tentative</code> as expected. With this fix, the monitored destination IP address correctly shows as <code>down</code> when unavailable, which results in the firewall correctly changing status to <code>tentative</code> .
79504	Fixed an issue where a passive M-100 appliance in a high availability (HA) configuration lost its device group and template configuration.
79279	Fixed an issue that caused an error to be displayed (<code>ntp-servers unexpected here. Discarding.</code>) when pushing a device group configuration through templates after a Panorama upgrade.
79278	Fixed an issue where the active device in a high availability configuration failed to generate tech support files due to a buffer limitation that could not accommodate the output from some commands. With this fix, the commands that prevent generation of tech support files have been removed so that reports are generated as expected.

Issue Identifier	Issue Description
79266	Fixed an issue where an administrator was unable to access the web interface or command line interface (CLI) when the schema file either did not exist or was empty (0 bytes). With this fix, a missing or empty schema file does not prevent administrators from accessing the web interface or CLI.
79046	Fixed an issue on an M-Series appliance running in Log Collector mode where log forwarding to an external syslog server stopped working after a Panorama commit when forwarding logs through TCP port 514 (default) instead of UDP port 514 (Device > Server Profiles > Syslog). With this fix, you no longer need to perform a Collector Group commit to resume log forwarding after a Panorama commit when the syslog server is configured to use TCP.
78511	Fixed an issue where the DHCP relay agent incorrectly set the gateway IP address (<i>giaddr</i>) value to zero (instead of the IP address of the ingress interface as defined in RFC 1542) when responding to DHCP requests.
78445	Fixed an issue where HTTP Header Logging was enabled for a URL Filtering profile (Objects > URL Filtering > URL Filtering profile > Settings) but HTTP headers were not correctly logged when the URL was too long to be captured in a single packet. With this fix, long multi-packet URLs are logged correctly.
78436	Fixed an issue where the management plane stopped responding when more than one process attempted to modify the device table during a configuration push from Panorama. With this fix, the device table is locked and modifiable by only one process at a time to avoid conflicting modifications.
78187	Fixed an intermittent issue with a system process (<i>all_task</i>) that caused a device to restart unexpectedly. This fix includes an adjustment to an internal timer to avoid these restarts.
77816	Fixed an intermittent issue where some Windows 7 GlobalProtect™ clients using two-factor authentication (LDAP and certificate) lost connection to the portal or gateway and could not reconnect due to a failed authentication with the error <code>Required client certificate is not found</code> even when the certificate was available.
77721	Fixed an issue on a PA-200 firewall where a reboot took much longer than expected (more than 20 minutes). This issue occurred when the Content Updates database was corrupted and updates did not stop or pause as expected to allow the reboot to take place. With this fix, the firewall reinitializes the database if it is corrupted to allow the Content Update and system reboot to proceed as expected.
76875	Fixed an issue where the dataplane rebooted when a process (<i>brdagent</i>) was terminated by the firewall in response to an out of memory condition. With the fix, dataplane reboots are no longer triggered by these out-of-memory events because the firewall no longer considers the <i>brdagent</i> process for termination when attempting to address an out-of-memory event.
76811	Fixed an issue where packet loss could occur with asymmetric traffic when two PA-4060 firewalls were set up as peers in a high availability (HA) active/active configuration. This issue occurred with VLAN-tagged traffic when jumbo frames processing was disabled and large non-jumbo frames passed over the HA3 link and became jumbo frames.
76781	Fixed an issue where a firewall incorrectly calculated packet length and TCP sequence due to a one-byte zero-window-probe packet when that packet was sent from one vsys to another.

Issue Identifier	Issue Description
76631	Fixed an issue on PA-7000 Series firewalls where the Log Processing Card (LPC) failed to resolve the FQDN of the syslog server. With this fix, the firewall will re-initiate the DNS lookup request until the lookup succeeds.
75803	Addressed an issue regarding how often password API keys are regenerated.
75677	Fixed a Panorama issue where clearing the setting Require SSL/TLS secured connection for a vsys-specific LDAP server profile (Templates > Device > Server Profiles > LDAP) displayed an error.
73443	Fixed an intermittent issue that resulted in corrupted forwarding entries on the offload processor.
73118	Fixed an issue on a PA-7050 firewall where the CLI output for the <code>show system logdb-quota</code> command showed zero disk usage on an LPC, indicating there were no logs even though logs were successfully collected. With this fix, results of the <code>show system logdb-quota</code> command are accurate.
72756	Fixed an intermittent issue where a race condition caused by multiple processes asynchronously attempting to retrieve the last saved configuration file caused Captive Portal or the FQDN refresh job to fail.
72371	When a custom QoS profile was enabled on an interface, the QoS statistics for the custom profile were instead displayed as the default QoS profile statistics. This issue has been resolved so QoS statistics are displayed correctly with the corresponding QoS profile (and for each class in the profile).
69837	In response to a rare issue where a PA-200 firewall stopped processing traffic, PAN-OS 6.1.4 and later releases included additional troubleshooting information and some modifications to error checking and counter processes to help prevent and troubleshoot the issue. With this fix in PAN-OS 6.1.7, those PAN-OS 6.1.4 modifications are replaced by an update to the third-party SDK that delivers a more complete solution to this issue.
69671	Fixed an issue on PA-7000 Series firewalls in a high availability (HA) configuration where the HA1 peer did not boot properly and caused both HA peers to come up in active-primary state even though one should have been in active-secondary state. With this fix, HA1 boots up correctly so that both firewalls are in their appropriate HA mode (one is active-primary and the other is active-secondary).
69132	Fixed an issue where occasional dataplane restarts occurred due to a kernel memory allocation failure.
68672	Added a fix to prevent using names for custom applications that have already been used to name internal Palo Alto Networks applications.
66681	Resolved a dataplane restart issue due to race conditions.
64531	Fixed an issue where a high availability (HA) failover occurred due to insufficient kernel memory on a PA-5000 Series firewall. With this fix, PA-5000 Series firewalls include some cache-flushing events and increased kernel memory to ensure sufficient kernel memory remains available for ping requests and keep-alive messages to avoid these HA failovers.
64266	Fixed a rare issue where certain processes (<code>l3svc</code> and <code>sslvpn</code>) stopped responding when a Content update and FQDN refresh occurred simultaneously.

PAN-OS 6.1.6 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.6 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).

Issue Identifier	Description
81500	Fixed an issue where a VM-Series firewall in a VMware NSX configuration running on an ESXi server restarted when a process (<i>all_task</i>) stopped responding.
80924	Fixed an issue where a GlobalProtect™ Large Scale VPN (LSVPN) satellite configuration caused the satellite firewall to Proxy ARP for the defined access route subnets on all logical and physical interfaces.
80592	Fixed an issue where firewalls in a high availability (HA) active/passive configuration did not sync the Dynamic Address Group when one of the firewalls stopped functioning and then changed to a functional state.
80408	Fixed an issue where, in some environments, new content updates could no longer be accommodated by the memory on the firewall that is allotted for these files due to a continually increasing number of applications in the updates. With this fix, allocated memory for content updates is increased so that continued growth of content updates will not prevent successful download and installation of those updates.
80318	Fixed an intermittent issue on a PA-7050 firewall where some packets were dropped during the initial session setup process. This issue occurred when two packets in the same session were sent almost simultaneously, causing the second of the two packets to get dropped.
79929	Fixed an issue where a process (<i>mprelay</i>) stopped responding and did not receive a refresh of the configuration when it restarted.
79709	Fixed an intermittent issue where ZIP processing may cause the dataplane to restart.
79522	Fixed an intermittent issue where a firewall with hardware offload enabled included an incorrect IP checksum value in outgoing NAT packets, which caused some packets to be dropped.
79511	Fixed an issue on Panorama where disabling the Share Unused Address and Service Objects with Devices option (Panorama > Setup > Management > Panorama Settings) when no Shared objects were configured caused a process to restart during a commit.
79478	Fixed an issue where the firewall connected directly to a directory server instead of the User-ID™ agent configured as an LDAP proxy. With this fix, the firewall correctly uses the User-ID agent when the agent is configured for use as an LDAP proxy.
79443	Fixed an issue in the web interface where, in some cases, the PHP session cookie (PHPSESSID) was not marked as secure.
79401	VM-1000-HV firewalls running on eight vCPUs did not save and display traffic and threat logs. With this fix, VM-1000-HV firewalls properly save and display the logs. This issue did not affect VM-Series firewalls running on two or four vCPUs.

Issue Identifier	Description
79382	Fixed an issue where IP address registration through the XML API failed to populate the Dynamic Address Group following an <code>AddrObjRefresh</code> job failure during a template commit from Panorama when the Force Template Values option was checked, resulting in an <code>Error: Failed to parse security policy.</code>
79367	Fixed an issue in PAN-OS where GlobalProtect clients experienced delays and intermittently failed to retrieve the gateway configuration for connecting to a GlobalProtect gateway when the firewall was in a high availability (HA) configuration and under a heavy load. This issue occurred due to an issue with the synchronization of HIP reports between gateways on HA peers when there was a high number of near-simultaneous GlobalProtect connection requests. With this fix, the sync process is modified so that GlobalProtect clients are able to download the configuration and connect to the network as expected even when multiple clients are attempting to connect at the same time.
79335	Fixed an issue where attempting to filter system logs using the log filter <code>Type equal globalprotect</code> did not work. A space was automatically added to the log filter, causing an error to be displayed.
79069	Improved the handling of login attempts for unknown usernames over SSH.
78646	Fixed an issue where a firewall replaced multibyte characters with a period character (.) when forwarding logs or event information to SNMP traps, to a syslog server, through email, or in scheduled log exports. This issue also occurred when exporting logs to CSV. With this fix, multibyte characters are forwarded and exported correctly with one exception: in PAN-OS 7.0.1, PA-7050 firewalls will still incorrectly replace multibyte characters with period characters when exporting logs to CSV.
78571	Fixed an intermittent issue where a firewall received a Virtual Systems license that allowed for a higher number of virtual systems than the maximum amount supported for the platform. With this fix, the licensed virtual systems activated on a firewall cannot be higher than the maximum amount of virtual systems supported on the device.
78343	Fixed an issue that occurred with decryption enabled, where some websites were not decrypted due to an issue with certificate serial numbers.
78321	Fixed an issue where the Captive Portal timeout value for a user was set incorrectly on the dataplane. With this fix, the dataplane is updated with the correct timeout value for all users.
78084	The output for the command <code>show log collector serial number</code> displayed different log data when executed on a primary-active Panorama than the output that was displayed when the command was executed from the secondary-passive Panorama. This issue is fixed so that the output for the command <code>show log collector serial number</code> correctly displays the latest log data for managed log collectors.
77784	Fixed an issue on Panorama where administrators were unable to filter Device Groups by tags in the commit window.
76648	Fixed an intermittent issue where logging in to Panorama through the web interface resulted in the display of empty (blank) web pages.
75758	Fixed an issue where the dataplane restarted on a PA-5000 Series firewall in a high availability (HA) cluster due to corruption of ARP packets.
75344	Fixed an issue where a memory process restarted and caused an invalid memory reference; the invalid memory reference resulted in a management plane restart.

Issue Identifier	Description
74609	Fixed an issue on a PA-5000 Series firewall where PREDICT sessions were handled by dataplane 0 (DPO) but the SIP parent sessions were on a different dataplane. With this fix, you can use the <code>set session filter-ip-proc-cpu dest-ip <IPaddr></code> CLI command to specify all destination SIP proxy IP addresses in a filter list on the firewall. You can then use the list to configure the firewall so that DPO receives and handles any inbound packet that is destined for any of the specified SIP proxy IP addresses.
73631	Fixed an issue where several NTP sync errors were displayed following a firewall software upgrade.
72153	Fixed an issue where the first SYN packet in a TCP connection that passed through two virtual systems did not reach the destination server. This occurred when one virtual system was using DNAT and the second was using SNAT and sessions were allocated on different dataplanes (DPs), with the first session on DPO.
70335	Fixed an issue where access routes from the GlobalProtect gateway could not be installed on a satellite when the tunnel monitor was enabled for a Large Scale VPN (LSVPN) and the tunnel monitor was in <code>wait recover</code> mode.
68904	Fixed an issue where a Collector Group commit triggered Log Collectors to send updates to Panorama deployed in a high availability (HA) configuration but the passive Panorama peer did not receive the updates. As a result, only the active Panorama peer updated the ring file, which caused a <code>Config mismatch</code> error in the Last Commit Status for the passive peer. With this fix, you can perform two consecutive Collector Group commits after making your changes to the Collector Group configuration to force the passive Panorama peer to accept updates and stay in sync with the active peer.
68215	Fixed a race condition that caused the User-ID process (<code>userid</code>) to stop responding.
66281	Fixed an issue where dynamic block lists were not refreshed as expected when enabling use of a proxy server.

PAN-OS 6.1.5 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.5 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).

Issue Identifier	Description
79381	Fixed an issue where a VM-Series firewall on a VMware ESXi server experienced degraded performance or interruptions in traffic when attempting to transfer large files through a GlobalProtect™ SSL tunnel. With this fix, the firewall passes large files without signs of degraded performance or interruptions in traffic flow.
79104	Fixed a rare issue on a PA-7050 firewall where the HA1 and HA1 backup links experienced heartbeat failures that caused split brain in a high availability (HA) configuration.
78652	Fixed a rare issue where a firewall dropped URL requests when the management plane (MP) URL <i>trie</i> (data structure) reached 100% capacity. With this fix, when the MP URL trie reaches 90% capacity, URLs in the cache are cleared until the MP URL trie utilizes only 50% of capacity so that the trie cannot reach maximum capacity and cause requests to be dropped.
78621	Fixed an issue that occurred when Chile adopted new official times and the official time for Continental Chile became UTC-03:00. A PA-200 firewall configured to use the Chile Continental time incorrectly continued to display the official time as UTC-04:00.
78448	Fixed an issue where a custom response page containing an invalid substring caused the process for communicating between the dataplane and management planes (<i>mrelay</i>) to stop responding when attempting to commit configuration changes.
78413	Fixed an issue on a PA-7050 firewall with multiple virtual systems where a memory leak was observed related to the First Packet Processor (FPP) management plane process when running the <code>show session meter</code> CLI command.
78346	Fixed an issue where, with Strip X-Forwarded-For (XFF) enabled (Device > Setup > Content-ID), the firewall stripped the XFF IP address and inserted spaces. With this fix, you can execute the <code>debug dataplane set x-fwd-for-enhanced</code> on CLI command to configure the firewall to replace the XFF IP address with <code>1.1.1.1</code> instead of spaces.
78304	A security-related fix was made to address a cross-site request forgery (CSRF) issue in the web interface.
78268	Fixed an issue where NAT IP addresses did not show up for related logs—listed in the bottom pane of the Detailed Log View for a Traffic log (Monitor > Logs > Traffic)—when viewing information for a log related to a NAT session Traffic log.
78211	Fixed an issue where a user was not matching correct security rules after logging out and back in due to a missing host information profile (HIP profile).

Issue Identifier	Description
78149	Fixed an issue where RADIUS authentication did not work when the RADIUS server profile was configured with an IPv6 address. This occurred when a RADIUS request attribute used for network access server (NAS) IP addresses was not handled correctly when using an IPv6 address. With this fix, RADIUS server profiles support IPv6 addresses.
77918	Fixed an issue on a WF-500 appliance where inconsequential network block device (NBD) error messages were sent to the serial management console each time a new sample was sent to WildFire™ for analysis; in some cases, more rapidly than the administrator could monitor or ignore the messages, making it difficult to manage the device. With this fix, these inconsequential error messages are no longer displayed on the console.
77907	Fixed an issue where log forwarding to a Log Collector did not stop as expected when executing the <code>request log-fwd-ctrl device <s/n> action stop</code> CLI command on Panorama™.
77763	Fixed an issue on a PA-7050 firewall where a floating IP address configured for port 24 on a Network Processing Card (NPC) did not respond correctly (regardless which slot you use for the NPC).
77749	Fixed an issue where clicking More to view the registered IP address under Policies > Security > Object > Address Groups resulted in an error.
77561	Fixed an issue where SSL decryption stopped working after signing approximately 1,500 certificates when using a Thales hardware security module (HSM). This issue occurred due to a <code>cert cache entry</code> memory leak. With this fix, the <code>cert cache entry</code> memory leak is eliminated and SSL decryption using Thales HSMs works as expected.
77548	Fixed an issue where changing the Configuration refresh interval on the Tunnel Settings tab (Network > GlobalProtect > Gateways > Satellite Configuration) did not update the Refresh Time as expected. With this fix, you can click Refresh GW Config (Network > IPSec Tunnels > Gateway Info) to update the Refresh Time without having to Reconnect to GW .
77477	Fixed an issue where a user was no longer able to connect to a GlobalProtect gateway that was deployed using Amazon Web Services (AWS) after the user had been connected for several hours and the user could not reconnect until the gateway was restarted. With this fix, users no longer lose their connection to the GlobalProtect gateway if they stay connected for several hours.
77413	Fixed an issue where the authentication process failed to parse the base Distinguished Name (DN) correctly when it contained a space (" ") character.
77307	Fixed an issue where the CLI seemed unresponsive after running the <code>show config diff</code> command due to the extended period of time it took to process and return results for a diff containing a large number of config changes. With this fix, the <code>show config diff</code> command returns results without any significant delay.
77283	Fixed an issue where the Threat Name did not display in the Detailed Log View when clicking on a related Threat log (listed in bottom pane of Detailed Log View) when viewing Detailed Log View for a Traffic log (Monitor > Logs > Traffic).
77264	Fixed an issue in Panorama where cloning a Scheduled Config Export file (Panorama > Scheduled Config Export) failed with the following error: 1- Failed to clone <code><SchedCfgExpName></code> . Cloning allowed only for a top level object.

Issue Identifier	Description
77170	Fixed an issue where no error messages were displayed during agentless User-ID™ configuration when attempting to specify a username that was not NTLM-compliant. With this fix, help strings are added in the web interface to help users create usernames that stay within NTLM parameters.
77163	Fixed an issue where the <code>/var/log/secure</code> log file inflated and consumed available disk space. With this fix, PAN-OS uses a log rotation function for this log file to avoid consuming more disk space than is necessary.
77148	Fixed an issue where the Panorama management server stopped responding after attempting to register IP addresses to a Dynamic Address Group when using the XML API without specifying the <code>target</code> option. With this fix, adding IP addresses to a Dynamic Address Group on Panorama using the XML API is successful even when not specifying the <code>target</code> option.
77065	Fixed an issue on PA-5060 firewalls running PAN-OS 6.1.0 or later releases where the NetFlow App-ID field for NetFlow packets with PAN-OS Field Type 56701 was set to null instead of to the appropriate application name, which prevented a NetFlow collector from gathering and displaying any useful NetFlow statistics. With this fix, all NetFlow packets have the correct application name in the NetFlow App-ID field.
77023	Fixed an issue where an administrator was sometimes disconnected from web interface due to a race condition caused by switching between log types and tabs within the Monitor tab.
76847	Fixed an issue where IKE phase 2 re-key was happening too frequently for an IPSec site-to-site VPN configured with tunnel monitoring on multiple Proxy IDs when QoS was enabled.
76759	Fixed an issue where an SSL scan of a WF-500 appliance returned SSLv3 connections and RC4 ciphers even though the WF-500 appliance no longer supports SSLv3. With this fix, the WF-500 appliance returns only TLSv1 connections.
76711	Fixed an issue where the dataplane stopped responding on a device using a shared gateway with Captive Portal in redirect mode.
76575	Fixed an issue on a PA-5000 Series firewall where an occasional inconsistency in the IPv6 neighbor cache on different dataplanes caused IPv6 traffic sent to certain hosts to get dropped. With this fix, the firewall keeps the IPv6 neighbor cache in sync between dataplanes so that IPv6 packets are not dropped.
76569	Fixed an issue where a GlobalProtect satellite was unable to connect to the gateway when the portal was configured using an FQDN instead of an actual IP address. With this fix, satellite devices can connect to the gateway when the portal gateway address is specified in FQDN format.
76256	Fixed an issue on an M-100 appliance where the exported device state configuration from a replaced firewall did not contain any data in the Shared policy and template directories after replacing the serial number (adding serial number for the new firewall in place of the old serial number).
76209	Fixed an issue where data displayed in network monitor graphs was not accurate due to an issue with internal rendering and summarizing of data. With this fix, values in the network monitor graphs are accurate.

Issue Identifier	Description
76083	Fixed an issue where no System logs were generated for failed login attempts using the CLI over an SSH connection. With this fix, additional System logs now provide visibility for failed logins to the management interface even if those attempts come from a CLI over an SSH connection.
76079	Fixed an issue on a PA-7050 firewall where Traffic logs on Advanced Mezzanine Cards (AMCs) could not be recovered after replacing a Log Processing Card (LPC). With this fix, a new CLI command (<code>request metadata-regenerate slot <slotnum></code>) is in place to retrieve logs from AMC disks after replacing LPCs.
75983	Fixed an issue in Panorama where an administrator logged in using RADIUS Vendor-Specific Attribute (VSA) authentication could not see virtual system information in the vsys column (Network > Interfaces) for interfaces that were configured as part of a virtual system; instead they would see a value of <code>none</code> in that column. With this fix, the vsys column correctly displays vsys information even if the administrator is logged in using RADIUS VSA authentication.
75907	Fixed an issue on firewalls running in a high availability (HA) active/active configuration where oversized files passed between peers caused commits to fail. With this fix, an HA peer checks that files do not exceed maximum size before sending them to the other peer to avoid these types of commit failures.
75881	Fixed an issue on a PA-5000 Series firewall where the management plane and dataplane restarted due to a race condition that occurred when the Enforce Symmetric Return option was enabled in the policy-based forwarding (PBF) rules (Policies > Policy Based Forwarding > Forwarding). This race condition caused inaccurate PBF <code>return-mac</code> <code>ager</code> lists, which caused the restarts. With this fix, the firewall retrieves and checks return MAC entries to avoid this race condition and associated restarts.
75825	Fixed a rare issue on a PA-5000 Series firewall where a race condition occurred between dataplanes 1 and 2 (DP1 and DP2) and dataplane 0 (DPO) that incorrectly caused a reset of the timeout value for parent sessions owned by DP1 and DP2 when creating predict sessions, which caused those parent sessions to time out prematurely. With this fix, the timeout for parent sessions is not changed when the predict sessions are created.
75744	Fixed an issue where a dataplane stopped responding after a commit that changed the interface index when high availability (HA) session packets were referencing that interface index using an interface pointer.
75238	Fixed an intermittent issue where the environment health monitoring process (<code>ehmon</code>) stopped responding when the firewall shut down. This issue has minimal impact because it occurs during a shutdown but, with this fix, the <code>ehmon</code> process shuts down gracefully during a shutdown event.
75104	Fixed an issue where, in some cases, VMware vCenter and ESXi servers configured as VM Information Sources did not reconnect to the firewall as expected after the servers were rebooted. With this fix, VMware vCenter and ESXi servers configured as VM Information Sources reconnect automatically after a reboot.
74998	Fixed an issue where the Palo Alto Networks Update Server was not correctly verified when a device used HTTPS with Verify Update Server Identity enabled (Device > Setup > Services > Global).
74959	Fixed an issue where the scheduled report did not match the custom report. With this fix, these reports match and display accurate data.

Issue Identifier	Description
74600	A security update was made to the OpenSSL package to address multiple vulnerabilities impacting the OpenSSL libraries.
74558	Fixed an issue on a PA-7050 firewall where, after upgrading to a PAN-OS 6.1 release, the post-upgrade autocommit failed when the high availability (HA) peer was still running a PAN-OS 6.0 release.
74333	Fixed an issue where incremental updates for new and updated registered IP addresses were failing when registration events were occurring through the XML API. With this fix, integrating the updates for registered IP addresses no longer fails when using the XML API.
73755	Fixed an issue where the firewall restarted when experiencing frequent restarts of the unified logon component that caused the NTLM process to stop responding. With this fix, the firewall no longer reboots when NTLM stops responding.
73693	Fixed an issue in Panorama where the Contact field for a Collector Group (Panorama > Collector Groups > Collector Group > Monitoring) would not accept any value that was not in an email address format (<name>@<company.org>). With this fix, the Contact field is no longer restricted to email addresses; the field will accept all regular text strings, such as phone numbers and URLs, in addition to email addresses.
73317	Fixed an issue where the System log displayed an IPv4 address for a firewall that was connected to an Active Directory (AD) server through a management port using an IPv6 address. For example: <code>ldap cfg <group_name> connected to server <IPv6 address>, initiated by: <IPv4 address></code> . With this fix, the appropriate IP address and format is displayed for the initiating device even when connected using an IPv6 address.
73177	Fixed an issue where redistributed Not-So-Stubby Area (NSSA) type 7 routes converted to NSSA type 5 routes were not flushed from the OSPF database quickly enough after the redistributing NSSA router went down. With this fix, the OSPF is flushed within the expected period of time so that routes that go down are not advertised as still available.
72969	Fixed an issue where a PDF Summary Report was generated in English even when the locale setting on the firewall was set to Japanese. With this fix, PDF Summary Reports are generated in the language associated with the locale setting specified on the firewall (Device > Setup > Management > General Settings > Locale).
72534	Fixed an issue where BGP aggregate routes were exported with the wrong next-hop when multiple peers were configured in the same peer group.
72530	Fixed an issue where interfaces on a passive device in a high availability (HA) configuration were physically brought up for a short time and then brought down again during bootup even though Passive Link State was set to shutdown (Active Passive Settings under Device > High Availability > General). (However, no packets were sent out and no packets received were processed during that time.) With this fix, the interfaces on the passive device stay down as expected during boot up unless Passive Link State is set to auto .
72445	*Fixed an issue where an administrator with read-only permissions could attempt to suspend local device from the web interface (Device > High Availability > Operational Commands); however, as expected, there was no effect if the read-only administrator confirmed this request when prompted. With this fix, the Operational Commands tab has been removed from view for read-only administrators.

Issue Identifier	Description
72396	Fixed an issue where a file hash containing capital letters failed to get processed when submitted to a WF-500 appliance using the XML API. With this fix, hashes are normalized before processing to prevent failures caused by capital letters.
71555	Fixed an issue where users were unable to check the configured quota on a Log Collector. With this fix, the <code>show log-diskquota-pct</code> CLI command is added so users can check the quota on Log Collectors.
71500	Fixed an issue where an administrator was unable to log in to an M-100 appliance due to an unresponsive management server.
71477	Fixed an issue where a firewall displayed false positive alerts for a TCP port scan when traffic was sent to a destination with only two alternating ports. With this fix, the TCP port scan logic is enhanced to prevent false positive alerts when only two alternating ports are used.
71459	Fixed an issue where <code>wildfire-upload-skip</code> actions were not logged when sending benign files for analysis if WildFire had already seen those files and the Report Benign Files option was disabled (Device > Setup > Wildfire > General Settings). With this fix, both <code>forward</code> and <code>wildfire-upload-skip</code> actions are logged in the Data Filtering log even when Report Benign Files option is disabled.
70537	Added a new debug CLI command (<code>debug dataplane internal pdt pci list</code>) to provide a dump of the peripheral component interconnect (PCI) when attempting to identify the root cause for the <code>data_plane_X: Startup Script Failure</code> error.
70410	Fixed an issue in Panorama where custom reports were not generated properly when selecting serial number (Device SN) option in the Group By field (Monitor > Manage Custom Reports > Custom Report > Report Setting). With this fix, custom reports that are grouped by serial number are generated correctly.
70144	Fixed an issue where a virtual system administrator did not get an application dependency warning as expected during a commit attempt when there was a conflict; this warning message only displayed for a superuser. With this fix, the application dependency warning is displayed when appropriate to virtual system administrators, in addition to superusers.
69391	Fixed an issue where a rule created based on a threat name in an Anti-Spyware profile was applied to all signatures. With this fix, a rule defined in an Anti-Spyware profile is applied only to the specified threat.
69051	Fixed an issue where the firewall failed to apply NAT within an H.225 packet for the IP address of a phone. With the fix, the firewall applies NAT as expected for the IP addresses of phones within H.225 Connect messages.
68537	Fixed an issue where a firewall stopped responding during the license installation process.
68508	Fixed an issue where the DHCP server sent DHCP lease offers on the wrong interface after a high availability (HA) failover due to interface IDs being out-of-sync on the HA peers.
65392	Fixed an issue where the log receiver stopped responding during a restart that happened at the same time that a NetFlow profile was removed from a security policy rule that was still processing traffic.

Issue Identifier	Description
64658	Fixed an issue where an administrator for a firewall running a PAN-OS 6.0 or earlier release set the Maximum Concurrent Sessions field for a DoS Protection profile (Objects > DoS Protection > DoS Protection Profile > Resources Protection) to a value higher than 65,535, which caused commit attempts to fail after upgrading to a PAN-OS 6.1 release due to a new maximum number of concurrent sessions allowed (65,535). With this fix, upgrading to PAN-OS 6.1.5 or later releases on a firewall that was previously configured to allow more than 65,535 concurrent sessions will not cause a problem when attempting to commit changes.
63854	Resolved an issue where a virtual systems administrator could not use the XML API to add IP address-to-username mappings.
63652	Fixed an issue where some files forwarded to WildFire were not uploaded successfully due to a CANCEL_OFFSET_NO_MATCH error. With this fix, the offset (caused by a buffer overload) is no longer an issue.
59666	Fixed a rare issue where a VM-Series firewall incorrectly identified a second or subsequent packet fragment as the first fragment to arrive, which resulted in dropped packets.



PAN-OS 6.1.4-h2 Addressed Issues

The following table contains the issue that was fixed in the PAN-OS® 6.1.4-h2 release for the WildFire™ cloud and WF-500 devices. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).

Issue Identifier	Description
79984	Addressed the VENOM vulnerability (CVE-2015-3456) affecting QEMU, a software component used in the WildFire malware analysis system. With this fix, the WF-500 appliance and WildFire cloud services are protected from the VENOM vulnerability.

PAN-OS 6.1.4 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.4 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).

Issue Identifier	Description
78272	Enhancements have been made to the WF-500 appliance to reduce incorrect malware verdicts for PDF files.
78206	Fixed an issue where a multi-dataplane platform did not properly free SSL Forward Proxy memory for SSL session-cache entries that included a username field that was parsed from a client certificate. With this fix, memory is freed up as expected for session-cache entries that include a username field parsed from a client certificate.
77707	Fixed an issue where Threat Map and Traffic Map were not appearing on the web interface under Monitor > App Scope > Threat Map or under Monitor > App Scope > Traffic Map .
76615	Fixed an issue on a PA-7050 firewall where running the <code>request system private-data-reset</code> command when there was a faulty disk drive on the Log Processing Card (LPC) caused an LPC failure during reboot.
76570	Fixed an issue where a commit failed when uppercase-to-lowercase transformation of group and user configuration objects was not performed uniformly for all objects. With this fix, all uppercase group and user configuration objects are transformed to lowercase characters as expected during configuration parsing.
76561	Fixed an issue where the DHCP relay agent dropped DHCPDISCOVER packets that the agent could not process due to multiple BOOTP flags. With this fix, the DHCP relay agent recognizes the first BOOTP flag in a DHCPDISCOVER packet and ignores any additional BOOTP flags that may exist (per RFC 1542) so that multiple BOOTP flags do not cause DHCPDISCOVER packets to be dropped.
76238	A security-related fix was made to address CVE-2015-1873.
76185	Fixed a rare issue where both devices in a high availability (HA) active/active configuration entered active-primary state when the two firewalls completed the boot process almost simultaneously.
76110	Fixed an issue where System logs were generated with failed network time protocol (NTP) sync events even though there was no NTP server configured on the firewall. With this fix, error logs no longer include false failure messages for NTP sync.
76099	Fixed an issue where the dataplane restarted on a PA-7050 firewall when there was a NAT rule configured to use dynamic IP that falls back to dynamic IP and port (DIPP) NAT.
76043	Fixed a memory allocation issue on the PA-7050 firewall that caused intermittent connectivity for sessions inspected using SSL Forward Proxy decryption. An update was made to increase the proxy memory pool for PA-7050 firewalls, to allow for more memory to be allocated for SSL Forward Proxy sessions.

Issue Identifier	Description
76007	Fixed an issue where an asymmetric path configured with the drop packet option no longer worked as expected after an upgrade to a PAN-OS 6.1 release from an earlier PAN-OS feature release (PAN-OS 6.0 or earlier).
75905	Fixed an issue where a firewall failed to download the BrightCloud database via proxy after upgrading to either PAN-OS 6.1.2 or PAN-OS 6.1.3.
75783	Fixed an issue where GlobalProtect™ agent software failed to upload successfully to Panorama. With this fix, you can successfully upload and save the GlobalProtect agent software to Panorama (Panorama > Device Deployment > GlobalProtect Client > Upload) and then activate the GlobalProtect Client using that file (Activate From File).
75740	Fixed an issue where the log-receiver crashed during a restart that happened at the same time that a NetFlow profile was removed from a security rule that was still processing traffic.
75701	Fixed an issue where values for data displayed in Network Monitor charts (Monitor > App Scope > Network Monitor) changed from kilobytes and megabytes (KB/MB) representation to bytes after upgrading to PAN-OS 6.1. With this fix, data displayed in charts is displayed using KB/MB values.
75534	Fixed an issue where the reportd process crashed when executing the <code>show query result id <last job id> skip 0</code> command.
75103	Fixed an issue where the administrator was not notified of a commit failure when exceeding the maximum number of policy-based forwarding (PBF) rules in the configuration. With this fix, an error will be displayed as expected if trying to commit a configuration when the number of PBF rules exceeds the maximum allowed limit.
74932	Fixed an issue where high availability (HA) failovers that occurred with simultaneous route advertisements caused a routing process to restart, which then caused the firewall to restart.
74914	Fixed an issue in an asymmetric path configuration where HTTP GET requests were successful even though the session matched a custom URL category configured with the block-url action. In addition to this fix, you must permit asymmetric traffic in your environment for the block page to display when expected: <ul style="list-style-type: none"> • Configure a Zone Protection profile with the Asymmetric Path set to bypass (Network > Network Profiles > Zone Protection > Packet Based Attack Protection > TCP Drop) and apply the profile to the ingress zone for the asymmetric traffic; or • Enable asymmetric bypass globally on the firewall with the following configure mode CLI command: <code>set deviceconfig setting tcp asymmetric-path bypass</code>.
74735	Fixed an issue where a PA-7050 dataplane restarted when attempting to process jumbo frame packets.
74511	Fixed an issue where static discard routes did not get redistributed using OSPF; the routes were not injected in the OSPF link-state database (LSDB). With this fix, static discard routes are injected into the LSDB and distributed using OSPF as expected.
74506	Fixed an issue where, in some cases after selecting 5 (default) in the Context drop-down of the Config Audit tab (Device (or Panorama) > Config Audit) and clicking Go , the web interface returned the <code>Preparing config audit results</code> message and then stopped responding. To work around this issue in PAN-OS 6.1.3 and earlier releases, close the web interface and log in again and, if performing another Config Audit, choose a Context value other than 5 .

Issue Identifier	Description
73878	Fixed an intermittent issue where BGP failed to redistribute the static discard routes as expected after a high availability (HA) failover.
73712	Fixed an issue where viewing the traffic map for outgoing traffic in the Application Command Center (ACC) displayed data using the source country filter instead of the destination country filter. With this fix, viewing outgoing traffic in the Traffic Map is correctly filtered using destination country .
73710	Fixed an issue where, in some circumstances, tags learned via a VM Information Source failed to be removed from an IP address on the firewall when a VM information source indicated that the tag needed to be removed.
73689	Fixed an issue where traffic interruptions occurred due to nested encoding (ZIP content within chunked encoding), which caused the <code>SML VM vChecks</code> buffer pool to overflow. With this fix, new checks have been added to prevent <code>SML VM vChecks</code> buffer leaks.
73605	Fixed an issue where the User-ID process became unresponsive when trying to acquire the same lock twice with the same thread while executing the <code>idmgr reset</code> command for type <code>user</code> .
73598	Fixed an issue where executing the <code>show resource limit session</code> command displayed <code>max session as 0</code> even though the device had the default configured for maximum number of sessions supported on the firewall.
73481	Fixed an issue where an administrator with appropriate Admin Role permissions was unable to download a PDF file of the App Scope report (Threat Monitor > App Scope).
73197	Fixed an issue where the <code>domain is invalid</code> error message was displayed when attempting to add a new domain to the LDAP server configuration (Device > Server Profiles > LDAP) when the domain name included special characters. With this fix, the LDAP Server profile accepts special characters for NetBIOS domain names.
73152	Fixed a rare issue where 0-byte traffic logs were unnecessarily generated on a PA-7050 firewall for failed attempts to establish a dynamic IP NAT session when the IP pool was running low on IP addresses during heavy traffic flow. With this fix, the unwanted 0-byte logs are no longer generated.
73116	Fixed an issue where a firewall was unable to fetch an external block list (EBL) that included a truncated URL in the HTTP GET request (URL was truncated due to special characters in the original URL). With this fix, URLs with special characters in the EBL successfully upload to the firewall (Objects > Dynamic Block Lists) and are accessible for use in security rules.
73060	Fixed an issue where web sites that were added to the list of cached servers excluded from decryption were incorrectly added to the list using the IP address and port of the SOCKS proxy when the firewall was between the clients and the proxy server. As a result, decryption was disabled for all subsequent sessions passing through that proxy server. With this fix, the actual hostname of the web site to be excluded is added to the exclude-cache list and traffic to sites not listed in the exclude-cache list continue to be decrypted as expected.
73058	Fixed an issue where source and destination fields in SNMP traps were not populated for traffic using IPv6 addresses. With this fix and Rev. B of the PAN-OS 6.1 Enterprise SNMP MIB modules , new IP version-neutral fields were added (<code>InetAddress</code> and <code>InetAddressType</code> in place of the <code>IpAddress</code> field) to fully support IPv6 addresses. (The <code>IpAddress</code> field is retained for backward compatibility but is deprecated; administrators are expected to transition to the new fields.)

Issue Identifier	Description
72820	Fixed an issue on a PA-7050 firewall where a memory leak was observed related to the First Packet Processor (FPP) management plane process.
72811	Fixed an issue on PA-500 firewalls where an unexpected refresh date and time was displayed for the dynamic block list when executing the <code>request system external-list show name</code> CLI command. With this fix, the correct time and date are displayed for the dynamic block list.
72801	Fixed an issue where no warning was issued for an interface configured with an invalid OSPF authentication profile. With this fix, an <code>authentication is invalid</code> error message is displayed when the name of an OSPF authentication profile has changed and needs to be updated for an OSPF interface (OSPF > Area > Interface).
72715	Fixed an issue where Panorama failed to acknowledge and display logs that were forwarded from managed firewalls after upgrading to Panorama 6.1.2 or Panorama 6.1.3. To work around this issue when running either of these two releases, add the firewalls as Collector Group Members of a collector group in Panorama (Panorama > Collector Groups > Device Log Forwarding).
72665	Fixed an issue where custom reports (Monitor > Manage Custom Reports) that use summary logs as their data source display only one report per calendar day (labeled with 23:00) when output is grouped by hour . In PAN-OS 6.1.3 and earlier releases, you can work around this issue by using traffic logs as the data source.
72119	Fixed an intermittent issue on VM-Series firewalls where GlobalProtect clients stopped connecting and displayed a <code>Connection Failed</code> error, possibly due to an <code>encap/decap</code> context leak. With this fix, the <code>encap/decap</code> context leak is no longer observed.
71940	Fixed an issue where the dataplane restarted when SSL Inbound Inspection was enabled due to a software buffer overflow condition. With this fix, the software buffer size is increased to avoid this overflow condition.
71934	Inline editing is supported only for objects that do not include complex fields (fields that can contain more than one value). You must use dialog editing to successfully modify objects that include one or more complex fields so this fix disabled inline editing for objects, such as Redistribution profiles, that contain complex fields. Inline editing is still available for objects that contain only simple fields (those that contain only simple values, such as a single string or integer).
71828	Fixed an issue where the management plane ran out of memory due to stalled processes related to exporting logs. With this fix, the scheduled log export jobs complete as expected.
71692	Fixed an intermittent issue where some nested user groups did not display in the User Groups window (Device > Local User Database > User Groups) due to missing short name values that are used to display the groups. With this fix, nested user groups retain their short name value and are displayed as expected in the User Groups window.
71611	Introduced a CLI command in response to an issue on PA-7000 Series firewalls where logs did not always get generated or forwarded as expected when DNS response times were too slow. If you are unable to correct DNS server issues to improve response time on your network, use the <code>debug management-server report-nameLookup</code> command to work around this issue by disabling DNS name lookups in reports.

Issue Identifier	Description
71609	Fixed an issue where attempts to add an email address (Device > Server Profiles > Email) that included any special characters resulted in an <code><email address> is invalid</code> error message. With this fix, you can add email addresses that contain special characters in the local portion of the address (in front of @) as specified in RFC 3696.
70919	Fixed an issue where the dataplane in a high availability (HA) active/active configuration restarted when a <code>session update/remove</code> message was received from the peer while the session was pending an FPGA result. With this fix, FPGA results are ignored if the system receives a <code>session update/remove</code> message while waiting for those results.
70719	Fixed an issue where a dataplane restarted due to an incorrect flow ID. With this fix, additional checks are in place to prevent the dataplane from restarting due to this issue.
70669	Fixed an issue where the User-ID process stopped responding due to bulk and incremental updates of terminal server users on the active-secondary device in a high availability (HA) active/active configuration.
70523	Fixed an issue where coverage information in a WildFire™ Analysis report displayed conflicting information for WildFire and content coverage. With this fix, columns are updated so that the Date Released column displays the date a WildFire signature was first released and the Content Version column is renamed to Latest Content Version and displays the most recent content release version containing that particular signature.
70431	Fixed an issue where a custom URL category with the name <code>any</code> caused unexpected results. With this fix, the name <code>any</code> is no longer allowed when creating a custom URL category (Objects > Custom Objects > URL Category).
69959	Fixed an issue where a shared gateway was missing from the drop-down when specifying an Action in the Forwarding tab of a Policy Based Forwarding Rule (Policies > Policy Base Forwarding) after upgrading from PAN-OS 4.1 to PAN-OS 5.0 or higher releases. The missing gateway was not available via the CLI, either. With this fix, all shared gateways used when specifying a forwarding action are preserved during the upgrade.
69837	In response to a rare issue where a PA-200 firewall stopped processing traffic, additional troubleshooting information and some modifications to error checking and counter processes were added to help prevent this event and identify the root cause if it reoccurs.
69802	Fixed an issue where the window that popped up when clicking Browse to select an Address for an Address Object (Objects > Address Groups > Address Group) could not be resized. With this fix, the Browse window can be resized as needed.
69649	Fixed an issue where an HA3 interface was displayed in the web interface on a PA-7050 firewall in high availability (HA) active/passive configuration. With this fix, the HA3 interface appears only in an active/active HA configuration as expected.
69543	Fixed an issue where only output for the first virtual system (vsys) was displayed for a configuration with multiple virtual systems when a vsys administrator with access rights to multiple virtual systems executed the <code>show arp all</code> command. With this change, a vsys administrator can correctly view the ARP table for the vsys specified in the <code>set system setting target-vsys</code> CLI command.
69324	Fixed an issue where a Log Collector group configured with <code>local</code> as the group name triggered a reboot loop. With this fix, <code>local</code> is no longer allowed for use as the name of a Log Collector group.

Issue Identifier	Description
69131	Fixed an issue where, on certain platforms, a commit job that was pushed when the management plane CPU was under heavy load caused the firewall to restart. With this fix, the commit process is modified to prevent it from causing a service interruption regardless of the CPU load at the time the commit is pushed.
68559	Fixed an issue where a URL containing other embedded URLs with encoding (such as a redirect) that was encountered during the Captive Portal authentication process caused a loop in the web browser that required the browser to be closed and restarted. With this fix, Captive Portal properly handles these URLs.
68557	Fixed an issue where a dataplane stopped responding when zeroes were added before the session ID when running the <code>show session all start-at <session-id></code> command.
67458	Fixed an issue where a dataplane failed to get IP pool information from a dynamic IP and port (DIPP) source network address translation (SNAT) rule with an interface IP address.
66406	Fixed an issue where the current application version was not displayed correctly for managed firewalls when the firewall did not have a Threat Prevention subscription.
59914	Fixed an issue where the firewall did not remove the <code>pan_task_x.log</code> or <code>.log.old</code> files as expected when executing the <code>debug dataplane packet-diag clear log log</code> command.

PAN-OS 6.1.3 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.3 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).

Issue Identifier	Description
75869	Fixed an issue where the dataplane on a PA-5000 Series firewall running PAN-OS 6.1.2 stopped responding when processing encapsulated traffic.
74663	Fixed an issue where a static address group that exceeded the 500 address-object limit caused the dataplane to restart when trying to commit after a push from Panorama. With this fix, a commit that is pushed from Panorama and includes more than 500 address objects in a static address group will fail with a limit constraint error rather than restart the dataplane.
74526	Fixed an issue where the members listed by the <code>show user group name</code> command failed to include members of nested groups when using LDAP to connect to a lightweight directory service (LDS) active directory (AD) with LDAP Server Settings Type set to other (Device > Server Profiles > LDAP). With this fix, all members are listed as expected when connected to LDS with LDAP Server Settings Type set to other .
74212	Fixed an issue where an administrator with superreader access could no longer access <code>set password</code> and <code>set cli</code> commands in operational mode after an upgrade to PAN-OS 6.0 and PAN-OS 6.1 release versions. With this fix, superreader administrators can execute these <code>set</code> commands in operational mode.
74187	Fixed an issue where a web browser stopped responding when trying to access a URL where the admin override password was configured but the password value was <code>NULL</code> . With this fix, the firewall returns an appropriate failure message if receiving a <code>NULL</code> value for admin password override.
74138	Fixed an issue where PA-7050 firewalls in a high availability (HA) configuration experienced packet buffer leaks in PAN-OS 6.0 or higher releases. One instance of this issue occurred when the interface tables on two HA devices were out of sync and HA session sync messages included an interface ID that did not exist on the receiving device. Another instance occurred when the interface configurations on two HA devices did not match. In a third instance, a packet buffer leak occurred when the interface IDs on the two firewalls did not match even though the same set of interfaces was configured on the HA devices. This issue also occurred during an upgrade from PAN-OS 6.0 to PAN-OS 6.1 due to interface ID mismatch during the period where two firewalls in an HA pair are not running the same software version. With this fix, packet buffer leaks caused by such interface ID mismatch are prevented.
74049	Fixed an issue where the dataplane intermittently restarted on a PA-5000 Series firewall under heavy load conditions. This fix raises the priority of system health monitor packets so that they do not get dropped and cause the device to restart when under a heavy traffic load.

Issue Identifier	Description
73813	When using the PAN-OS CLI in configuration mode, the CLI command <code>show predefined signature</code> incorrectly displayed App-ID signatures and patterns for some predefined applications. The <code>signature</code> command option has been removed and the command <code>show predefined</code> now correctly displays application information, but does not display the App-ID signature and pattern.
73690	Fixed an issue where entering the <code>clear session all filter application dns</code> command on one dataplane incorrectly cleared the web-browsing session on the other dataplane. With this fix, the <code>clear session all filter application dns</code> command clears DNS sessions only on the dataplane on which the command is executed.
73630	Fixed an issue where an internal communication failure occurred when an internal virtual router interface tag (VR-ID) was updated while executing the <code>debug device-server reset id-manager type</code> command but the DHCP client and server were unaware of the change. With this fix, the DHCP client and server are aware of the VR-ID change and resolve the communication fault.
73337	Fixed an issue where a VM-Series firewall with a VPN configuration restarted due to a buffer overflow caused by a race condition.
73309	Attempting to use the web interface or CLI to upload a WildFire™ content release to Panorama displayed an error (Device > Dynamic Updates > WildFire). This issue has been fixed so that WildFire content updates can be uploaded successfully to Panorama.
73193	Fixed an issue where System, Config, and Threat (except URL) logs were forwarded to a syslog server as expected but Traffic and URL Threat logs were no longer forwarded after an upgrade from a PAN-OS 6.0 release version to a PAN-OS 6.1 release version. With this fix, all logs are forwarded to the syslog server as expected.
73180	Fixed an issue where, with Strip X-Forwarded-For (XFF) enabled under Device > Setup > Content-ID , an X-Forwarded-For IP address was not stripped before the packet was forwarded because the XFF header was split into two TCP segments due to an unusually long HTTP GET request. With this fix, the XFF field is stripped as expected when the header is split across two or more packets.
73109	Fixed an issue where an incorrect port mapping configuration caused packet loss on a PA-3060 firewall configured with Aggregated Ethernet (AE) interfaces 3 and 4.
73089	Fixed an issue where sender and recipient email addresses for some SMTP and POP3 sessions were not captured in WildFire Submission logs.
73071	Fixed an issue where the firewall incorrectly sent duplicate SYN packets for ftp-data sessions.
73068	Fixed an issue where a warning for application dependencies was displayed when committing a new or modified interzone security policy. With this fix, interzone security policy changes do not trigger the application dependency warning when committing configuration changes.
73045	Fixed an issue where the configuration daemon restarted while editing the candidate configuration, causing uncommitted changes to be lost.
73017	Fixed an issue where an autocommit failed on firewalls managed by Panorama running a PAN-OS 6.1 release version after upgrading the firewalls from a PAN-OS 5.0 release version to a PAN-OS 6.0 release version.

Issue Identifier	Description
72915	Fixed an issue where attempts to change the virtual system (vsys) configured for a virtual router (Network > Virtual Routers) failed when the Language Preference in the web interface was set to Japanese.
72897	Fixed an issue where a change to the IP address for an interface address object (Objects > Addresses) did not display properly for VPN and routing use (Network > Interfaces).
72859	Fixed an issue where some Threat logs did not display the correct direction for some entries after upgrading to PAN-OS 6.0 or PAN-OS 6.1 releases when policy-based forwarding (PBF) was configured. With this fix, the transmission direction for threat log entries is reported correctly when PBF is configured.
72825	Fixed an issue where traffic interruptions for various traffic patterns occurred when data was not released after packet processing. This caused Vchecks to remain allocated for an extended period of time, which depleted the buffer pool. With this fix, the Vcheck offset is modified so that data can be released and processed at a later time and avoid traffic interruptions.
72763	Fixed an issue where HA3 packet forwarding failed in a high availability (HA) active/active configuration when using an Aggregate Ethernet (AE) subinterface to send and receive traffic.
72741	Fixed an intermittent loss of DNS traffic that occurred when the second of two UDP packets was dropped if it arrived at the firewall immediately after the first packet and before the UDP session could be established. With this fix, the new UDP session is created before the second packet is processed so packets are not dropped.
72737	Fixed a memory corruption issue that caused the dataplane to restart when SSL decryption was enabled.
72730	Fixed an issue where it was possible for a firewall under heavy load conditions to send malformed BGP keep-alive messages to a BGP neighbor, causing the BGP neighbor to flap.
72662	In response to an issue where a web server process stopped responding, a check was added to help prevent further instances of this issue.
72582	Fixed an issue where requesting a Scheduled Log Export failed when specifying FTP and including special characters in the password (Device > Scheduled Log Export). With this fix, special characters in passwords can be used when configuring a Scheduled Log Export using FTP.
72536	Fixed an issue where packet buffers leaked when a firewall that had SSL Inbound Inspection enabled attempted to block a connection and send TCP RST packets to the connection endpoints. With this fix, TCP RST packets sent by the firewall to the connection endpoints no longer cause buffers to leak when SSL Inbound Inspection is enabled.
72092	Addressed an LSVPN issue where routes advertised by GlobalProtect™ satellites were not installed in a GlobalProtect gateway routing table. This issue has been resolved so that the GlobalProtect gateway correctly accepts routes from GlobalProtect satellites.

Issue Identifier	Description
71326	Fixed an issue where entering the <code>debug user-id clear registered-ip all</code> command in shared mode (accessed by executing the <code>set system setting target-vsyst none</code> command, where <code>none</code> specifies all virtual systems) did not clear all registered IP addresses from all virtual systems. The workaround for this issue requires executing the command one time for each virtual system. With this fix, execute the <code>debug user-id clear registered-ip all</code> command in shared mode one time to clear all registered IP addresses in all virtual systems.
71262	When two M-100 appliances were in a high availability (HA) active/passive configuration, memory usage for the passive appliance increased significantly compared to the memory usage for the active appliance. This was due to a management process memory leak on the passive device and the issue is fixed.
71040	Resolved an issue that caused SFP+ ports to hang following a restart and the ports continued to stay in down state.
70996	When Panorama was used to manage a firewall with a single virtual system, an Email server profile created by an administrator with the Device Groups and Templates role was stored in the <code>vsys1</code> location. When this Email server profile was referenced in a Log Forwarding profile within a specific Device Group, the Device Group commit failed with an invalid reference error. With this fix, when an administrator with the Device Groups and Templates role creates an Email server profile, the profile is saved in the Shared location on Panorama instead of <code>vsys1</code> and the Device Group commit is successful.
70902	Fixed an issue where importing a certificate into Panorama failed when the certificate filename included a space. With this fix, certificates with a space in the filename are successfully imported into Panorama.
70887	Fixed an issue where clicking the More link to view the registered IP address under Object > Address Groups resulted in an error if the name of a Dynamic Address Group included a space. With this fix, spaces in Dynamic Address Group names no longer cause an error when displaying the IP address.
70816	Fixed an issue where an <code>Invalid syntax error (not a valid source IP address)</code> was displayed when running certain commands (<code>clear session all</code> , <code>set application dump</code> , <code>test decryption-policy-match</code>) after initiating a filtering session based on an IPv6 address. IPv6 address validation now works correctly.
70544	A dataplane restart occurred when the SSL Decryption Opt-out Page was enabled (to notify users that SSL connections are decrypted), the RC4 cipher was enforced, and a long URL was accessed. This issue has been fixed so that the dataplane does not restart when the SSL Decryption Opt-out Page is enabled.
70304	Resolved an issue where a race condition could occur if new security policy rules were matched to existing sessions when Rematch Sessions (Device > Setup > Session) was enabled.
70295	Fixed an issue where a commit failed when an Aggregate Ethernet (AE) subinterface with DHCP client enabled was used for an IKE gateway configuration (Network > Network Profiles > IKE Gateway).
70075	Fixed an issue where a lack of content resources on a PA-3000 Series firewall caused some applications to be incorrectly identified or even fail. This fix ensures adequate resources are available for identifying and supporting all traffic sessions.

Issue Identifier	Description
70036	Fixed an issue where the web interface displayed partial or no results for report requests. With this fix, report requests are completed properly and results are displayed as expected.
69900	Fixed an issue where the tech support file did not contain some expected files, including /var/log files.
69409	Fixed an issue where a security policy rule containing two nearly identical rules (the only exception that the first rule contained a custom URL category with no specified URLs) prevented some applications from matching the appropriate rule. With this fix, applications match the correct rules and security policy rules are enforced as expected even if an empty custom URL category is added to a rule.
69266	Fixed an issue where queries were not saved when clicking OK when configuring Botnet reports after an upgrade to PAN-OS 6.0 and PAN-OS 6.1 release versions. With this fix, queries built under Monitor > Botnet > Report Setting in the web interface are saved when clicking OK and filters work as expected when running the Botnet report. As a workaround, you can build the desired query in the web interface but, before clicking OK , copy the query text and enter it in the CLI using the <code>set shared botnet report query</code> command (the query then displays as a saved query in the web interface).
69242	When an administrator failed to authenticate using the web interface, firewall System logs did not display the administrator's source IP address. Updates have been made so that a failed authentication on the web interface is logged with two entries. One entry is logged as a <code>general</code> event and displays only the username of the administrator who failed authentication. The other entry is logged as an <code>auth-fail</code> event and displays both the username and source IP address for the administrator who failed authentication.
69178	Fixed an issue where the DNS Proxy service was aborted when the file descriptors for TCP-based DNS request sessions were prematurely closed. With this fix, TCP-based DNS request file descriptors are allowed to age out and be deselected when no longer needed.
68770	Fixed an issue where a working IPSec tunnel would not reestablish after a NAT configuration was removed. With this fix, IPSec tunnels will successfully reestablish in response to the removal of NAT along the IPSec tunnel path.
67930	Fixed an issue where an update to a stale IPv6 neighbor entry caused a dataplane restart.
67709	Fixed an issue where a context switch over to a firewall in Panorama followed by a response page import attempt (Device > Response Pages) resulted in a failed import and displayed a misleading <code>Session timed out</code> error. With this fix, response page import requests after a context switch in Panorama are successful.
67523	Fixed an issue where the second pair of Aggregate Ethernet (AE) interface ports did not stay down when both ports on the first AE interface went down. This issue occurred on a virtual wire (vwire) with two AE interfaces that had link-state-pass-through enabled and where both ports on one AE interface went down. With this fix, when both ports on one AE interface go down, the second AE interface ports go down and remain in powered down state until the first AE link recovers.

Issue Identifier	Description
67515	Fixed an issue where clicking the OK and Cancel buttons did not result in the appropriate action when responding to an error message received after attempting to create an address object with the same name as an existing address object (Objects > Addresses). With this fix, clicking the OK or Cancel buttons in response to the error message works as expected; clicking OK allows you to continue the process and choose a different name while clicking Cancel exits the address object creation process.
67029	Fixed an issue where a large number of <code>ifInErrors</code> incorrectly warned of hardware issues after an upgrade to PAN-OS 6.0 or PAN-OS 6.1 release versions. Received counters now correctly differentiate between errors to avoid misleading warnings about hardware.
66113	Fixed an issue where adding a large number of groups and users to the allow list in the authentication profile resulted in longer than expected commit times. With this fix, the time it takes to commit changes to the configuration is reasonable even when an allow list contains a large number of groups and users.
65553	The option to Highlight Unused Rules did not work as expected for NAT policies. The expected behavior is for rules that are not being matched to traffic to show as highlighted; in this case, a rule that was not being matched to any traffic was not displayed as highlighted. This has been fixed so that NAT rules that do no match to any traffic are correctly shown as highlighted (Policies > NAT).
64887	Fixed an issue on a PA-7050 firewall where some traffic was dropped after a configuration commit that included a change to the interface configuration. With this fix, the firewall updates current available memory as expected when changes to the interface configuration are committed. Without this fix, you can work around the issue by committing a security policy change following any commit that includes changes to the interface configuration, which prompts the firewall to update current available memory settings.
62375	The GoDaddy root certificate authority (CA) was missing from the list of trusted certificate authorities. When SSL decryption was configured, sites using the GoDaddy root certificate authority were displayed as not trusted. With this fix, the GoDaddy Root Certificate Authority - G2 is included in the list of trusted CAs.

PAN-OS 6.1.2 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.2 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).

Issue Identifier	Description
73790	Additional security-related enhancements were made to support frame-busting for the firewall web interface, in order to prevent framing of web interface elements.
73757	A security-related fix was made to enforce character encoding specified in HTTP headers due to CWE-116: Improper Encoding or Escaping of Output .
73638	A security-related fix was made to address issues related to HTML encoding.
73594	When you extracted the image for the VM-Series NSX edition firewall from the zip file, the VF/DVMK were labeled ESX instead of NSX. This naming error has been fixed.
73111	Dataplane restarts were caused by a race condition between dataplane packet processes, where the session resource allocation became out of sync between central processing units (CPUs). A fix was added to keep session resource allocation in sync between dataplane processes.
72658	Japanese characters were not displaying correctly when the App Scope Summary was exported as a PDF. This issue has been fixed so that exporting a PDF of the App Scope Summary page displays characters correctly when the language preference is set to Japanese.
72544	A security-related fix was made to address CVE-2014-8730. For additional information, refer to the PAN-SA-2014-0224 security advisory on the Palo Alto Networks Security Advisories web site at https://securityadvisories.paloaltonetworks.com .
72241	Following an upgrade, attempting to perform a high availability (HA) configuration sync between two HA peers in an active/passive or active/active deployment did not sync correctly. This issue has been fixed so that HA peers will sync correctly following an upgrade.
72115	When the web interface was set to display in any language other than English, service routes to specify how the firewall communicates with other servers or devices could not be configured (Device > Setup > Services > Service Route Configuration). This issue has been fixed so that service routes can be configured and work correctly when the web interface is set to any language preference.
72068	If a firewall with Open Shortest Path First (OSPF) enabled was then restarted, a flapping condition was seen between the firewall and the adjacent OSPF neighbor, and a new OSPF election was forced for the firewall. This issue has been fixed so that following a firewall restart, any OSPF adjacency remains established.
71951	After restarting a PA-7050 firewall, a longer than expected period of time was necessary for an autocommit to complete and for the firewall to begin passing traffic. This issue was seen when the PA-7050 firewall had a large number of interfaces and address objects configured. An enhancement has been made to speed up the restart process.

Issue Identifier	Description
71939	Addressed an issue where enabling a second Network Processing Card (NPC) on a PA-7050 firewall resulted in URL packets being dropped by the second NPC and URL lookups could fail. This issue has been fixed so that URL lookups are performed correctly and web pages load quickly.
71893	When a custom URL category was selected as matching criteria for a QoS policy, other traffic besides that defined in the custom URL category was receiving QoS treatment. This has been fixed so that when a custom URL category is configured in a QoS policy, only the websites in that category receive QoS treatment.
71861	A passive device in an HA setup configured with Link Aggregation Control Protocol (LACP) interfaces was generating logs showing link states every five minutes. This issue has been resolved so that devices in a passive, suspended, or non-functional state do not generate logs.
71850	Changing the IP address for a log card interface on a PA-7050 firewall caused an issue where traffic log forwarded to syslog servers stopped until the firewall was restarted. This was due to an issue where the firewall sent out traffic using an internal IP address (which was recognized as an invalid source IP by devices intermediate to the firewall and the syslog server) following a change to the log card interface IP address. This issue has been fixed so that changing the IP address for a log card interface does not cause the firewall to send out traffic using an internal IP address.
71688	On a PA-7050 firewall with OSPF enabled, a restart caused OSPF neighbor adjacency states to flap. This issue was caused by an incorrect slot number setting on the Network Processing Card (NPC) for the session owner. With this fix, the NPC slot number for the session owner is properly selected and OSPF neighbor adjacency is established.
71634	Enhancements have been made to the WildFire™ appliance to reduce incorrect malware verdicts for Shockwave Flash (SWF) files, that were sometimes seen after upgrading the appliance and the firewall to PAN-OS 6.1 releases.
71604	When an SNMP server polled the firewall, the status for interfaces that were not configured was shown as up. An SNMP poll now correctly shows the status for interfaces that were not configured as down.
71553	Fixed an issue where dataplane processes restarted when handling SSL Decryption sessions during high availability (HA) message updates. The fix for this issue included the addition of a global counter.
71521	Addressed an issue where back-end process restarts caused the dataplane to restart. This was due to recursive functions consuming too much stack memory, making it possible for a certain traffic pattern (single byte HTTP chunked encoding) to result in a restart.
71512	A fix was made to add frame-busting to the firewall web interface to prevent framing of web interface elements.
71503	Addressed an incorrect file permissions issue in the web interface.
71486	A security-related fix was made to address an issue with user input sanitization to prevent Cross-Site Scripting (XSS) attacks against the web interface.

Issue Identifier	Description
71464	If a client initiates a Point-to-point protocol over Ethernet (PPPOE) session, an issue was seen when a server responds to the client with a PPOE Active Discovery Offer (PADO) packet that was greater in size than the maximum transmission unit (MTU) of the firewall interface. In this case, the PADO packet was dropped. This issue has been addressed so that PADO packets are handled correctly by the firewall, including when the size of the packet is greater than the MTU for the firewall interface.
71408	An error was displayed on the WildFire portal when downloading a WildFire Analysis Report as a PDF. This issue has been fixed so that using the option to download a WildFire Analysis Report as a PDF works correctly and does not display an error.
71333	In a high availability (HA) active/active configuration with an IPSec tunnel configured to terminate on a floating IP address, Encapsulating Security Payload (ESP) was performed by the device that did not own the floating IP address. The encapsulated packets failed the IPSec anti-replay check on the remote end of the IPSec tunnel and were discarded. With this fix, packets are always sent to the owner of the floating IP address to be encapsulated.
71321	Removed support for SSL 3.0 from the GlobalProtect™ gateway, GlobalProtect portal, and Captive Portal due to CVE-2014-3566 (POODLE).
71320	Removed support for SSL 3.0 from the web interface due to CVE-2014-3566 (POODLE).
71273	A security-related fix was made in PAN-OS to address issues related to parsing XML data.
71199	In a Large Scale VPN (LSVPN) setup, a GlobalProtect satellite reconnecting to a GlobalProtect gateway after receiving a different IP address, changed the GlobalProtect routing metrics when installing the gateway access routes into the satellite routing table. With this fix, the original gateway routing priority is restored when the GlobalProtect satellite reconnects to the GlobalProtect gateway with a different IP address.
71148	When attempting to add an address to an address group using the Panorama web interface, filtering for the address returned no results even though the address object did exist and was displayed as configured on the Objects > Addresses page. Additionally, filtering for the same address object when attempting to add the address to a security rule displayed different results for the address object name. This issue has been resolved so that filtering for an address correctly displays any configured address objects, and so that address object names are displayed consistently.
70920	License expiration dates are now enforced on all firewalls according to Coordinated Universal Time (UTC), regardless of the time zone configured for the firewall. This update resolves conflicts between local time zones and license expiration dates, specifically addressing conflicts due to the Daylight saving time (DST) transition.
70903	Fixed an issue where SNMP traps from some firewalls were not parsed correctly by the SNMP manager.
70837	VM Information Sources with names containing a space character were not handled correctly, and caused VM information retrieval from Amazon Web Services (AWS) to fail. This issue has been fixed so that VM Information Sources configured with a space character used in the Name field are handled correctly (Device > VM Information Sources).
70820	Addressed an issue for PA-7050 firewalls, where Real-time Transport Protocol (RTP) predict sessions remained in the Opened session state and did not become an active session. This caused the RTP packets to not merge correctly with the predict session and the packets were dropped if they did not specifically match to an allow policy.

Issue Identifier	Description
70706	When configured in a high availability (HA) active/passive configuration, an M-100 appliance could not be accessed using the web interface or the command line interface (CLI). In this case, a restart was required to gain access to the appliance. This issue has been fixed so that an M-100 in an HA active/passive configuration can be accessed correctly by an administrator using the web interface or CLI.
70383	When using the Panorama XML API to register an IP address to a Dynamic Address Group on a targeted firewall, an error was displayed that the user was not authorized to perform the operation. This issue has been resolved so that using the XML API to register an IP address to a Dynamic Address Group on the firewall results in the firewall correctly registering the IP address and updating the membership information for the dynamic address group.
70303	When attempting to create a custom spyware signature, using the Browse option to browse for and add threats did not correctly open the Spyware Browser ; instead, selecting Browse caused the Custom Spyware Signature dialog to close completely (Objects > Custom Objects > Spyware). This issue has been fixed so that selecting Browse correctly opens the Spyware Browser , and you can then select threats from the browser to be added as conditions for your custom signature.
70302	This fix addresses an issue where the autocommit process failed after upgrading a PAN-OS 5000 Series firewall or a PA-7050 firewall to a PAN-OS 6.1 release.
70150	Resolved an issue where Simple Network Management Protocol (SNMP) traps were not correctly sent to the SNMP trap destinations following a software upgrade. This issue is fixed so that SNMP traps are generated and correctly sent to SNMP trap destinations after performing an upgrade.
69934	Fixed an issue where an active File Transfer Protocol (FTP) connection failed when enabled with Source Network Address Translation (NAT) using a dynamic IP pool. This issue was due to the FTP control channel and the FTP data channel using different source IP addresses and the following error was displayed for the client: 500 Illegal PORT command.
69737	On platforms with multiple dataplanes, stale IPv6 neighbor entries were not removed and replaced with new IPv6 neighbor entries when the IPv6 neighbor table threshold was reached. This issue has been fixed so that stale IPv6 neighbor entries are correctly removed when the table threshold is reached. Additionally, for both platforms with multiple dataplanes and platforms with a single dataplane, once the table threshold of 70% is reached, a check is now made every 20 minutes to remove entries which have been stale for more than 10 minutes (this check was previously performed every hour).
69528	A fix was made so that in an environment where two virtual systems are configured as User-ID collectors for each other, and with captive portal enabled, IP address to username mappings are correctly refreshed among the virtual systems. The fix ensures that users are correctly prompted with the captive portal web page following a timeout.
69191	Addressed an issue where simultaneous downloads of the GlobalProtect installation program caused SSL-based VPN to fail.

Issue Identifier	Description
68812	In a Large-Scale VPN (LSVPN) configuration, where a GlobalProtect gateway and satellite resided behind a NAT device, the satellite incorrectly attempted to send Encapsulated Security Payload (ESP) packets to the original IP address configured as the gateway interface instead of to the external gateway specified in the satellite configuration for the GlobalProtect portal (Network > GlobalProtect Portal > Satellite Configuration). In this case, the ESP packets could not reach the gateway and tunnel traffic failed. With this fix, the GlobalProtect satellite correctly sends ESP packets to the external gateway specified for the satellite in the GlobalProtect portal configuration.
68764	When a proxy server is configured on the firewall, the proxy settings were not used and DNS resolution was requested to resolve service.brightcloud.com. After the fix, the connection request by the firewall to BrightCloud is always forwarded to the proxy.
68560	Addressed an issue where vulnerabilities were logged as unknown when an ampersand character (&) was used in the Comment field when creating a custom vulnerability object. Using the ampersand character in the Comment field when creating a custom vulnerability object is supported, and does not cause the vulnerability to display as unknown.
68430	The dataplane restarted unexpectedly due to a lack of memory. An update has been made to provide additional debug information for this issue.
68329	An option was added for VM-Series firewalls to provide administrators the capability to change socket buffer depth, in order to accommodate different requirements for packet loss and throughput.
67885	Panorama predefined reports for vulnerabilities were inconsistent with the predefined report for vulnerabilities on the managed firewall. This issue has been addressed so that reports are correctly synchronized between Panorama and managed devices.
67861	Following an upgrade to PAN-OS 6.0 releases, virtual wire interfaces went down after restarting the firewall. This issue has been fixed so that the status for virtual wire interfaces is no longer down after upgrading to a PAN-OS 6.0 release and restarting the firewall.
67719	The management interface was not receiving IPv6 connections for traffic from the dataplane when the firewall was in Layer 2 mode. An update was made to the MAC address learning process so that the Management interface receives IPv6 traffic from the dataplane when the firewall is in Layer 2 mode.
65553	The option to Highlight Unused Rules did not work as expected for NAT policies. The expected behavior is for rules which are not being matched to traffic to show as highlighted; in this case, a rule which was not being matched to any traffic was not displayed as highlighted. This has been fixed so that NAT rules which do no match to any traffic are correctly shown as highlighted (Policies > NAT).
61201	Scheduled email reports were not being delivered, though the reports were generating and displaying correctly on the Monitor tab on the web interface. This issue was due to a memory leak for a back-end process that maintains configuration information for the firewall. This issue has been fixed so that scheduled email reports are correctly delivered to email.
55249	You can now run the CLI command <code>test <feature></code> for the following features: botnet, cp-policy-match, custom-url, data-filtering, decryption-policy-match, dns-proxy, dos-policy-match, global-protect-mdm, global-protect-satellite, nat-policy-match, nd, pbf-policy-match, pppoe, qos-policy-match, routing, scp-server-connection, security-policy-match, stats-service, tag-filter, url, url-info-cloud, url-info-host, user-id, vpn, wildfire.

PAN-OS 6.1.1 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.1 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).

Issue Identifier	Issue Description
71618	Dataplane process restarts resulted in a dataplane restart. Improvements have been made to help prevent dataplane processes from restarting.
70588	Fixed an issue that occurred in cases where no client certificate is present; a browser with Transport Layer Security (TLS) 1.2 enforced could not access the GlobalProtect™ portal login page.
70499	Fixed an issue where traffic matched to a predict session and then converted to a flow session was then being incorrectly matched to security policies where the only matching criteria defined in the policy was a custom application. A fix was made to perform a second policy lookup after predict session traffic is converted to flow session traffic.
70459	Addressed an issue where attempting to use the Panorama XML API to request a tech support file for a managed device returned the tech support file for Panorama. An update was made so that an error is displayed if attempting to use the Panorama XML API to retrieve a tech support file for a managed device and the workaround to this issue is to download a tech support file from a managed device directly from the device.
70193	In PAN-OS 6.1.0, a custom HIP check was incorrectly matching to traffic if no processes defined in the custom check's Process List were running on the client system. Custom checks also incorrectly passed (meaning the check did not match to traffic) if all processes defined in the Process List were running on the client system. An update was made so that custom checks are matched correctly to client traffic depending on the status of the processes defined in the Process List: <ul style="list-style-type: none">• A custom check does not match to client traffic when all processes defined in the Process List are found to not be running on the client system.• A custom check matches to client traffic when at least one process (or more) defined in the Process is found to be running on the client system.
70165	Fixed an issue for PA-7050 firewalls in a high availability (HA) active/active configuration, where IPv6 fragments could cause a Network Processing Card (NPC) to restart.
70151	The firewall web interface could not be accessed using a Chrome browser following an installation of the Microsoft upgrade KB2998527. This issue has been fixed; as workaround for Chrome, you can also update your Chrome browser to the latest version.
69956	Fixed an issue for PA-5000 Series devices, where NetFlow information for some sessions was not being forwarded due to a session ID format change.

Issue Identifier	Issue Description
69725	Fixed an issue where a Log Collector running a PAN-OS 6.0 release did not correctly receive NTP server configuration settings when they were pushed from Panorama when Panorama was running PAN-OS 6.1.0. With this fix, NTP server configuration settings are successfully pushed from Panorama running a PAN-OS 6.1.1 or later release to Log Collectors that are still running a PAN-OS 6.0 release.
69598	Fixed an issue where an autocommit failed following an upgrade to PAN-OS 6.1.0 when Aggregate Ethernet (AE) interfaces were previously configured without defining an interface type (only possible when using the CLI; the web interface requires the interface type to be defined). With this fix, AE interfaces without an interface type specified (value is <code>null</code>) prior to an upgrade to PAN-OS 6.1.1 or later releases no longer cause autocommits to fail. However, when possible, administrators should set the interface type (HA, Layer 2, Layer 3, or virtual-wire) for any AE interfaces where one is not already specified.
69311	Using the command <code>scp export log traffic max-log-count <value></code> with the <code>value</code> variable set to a number greater than 1 million logs was displaying inconsistent results. This was due to the query timeout being 20 minutes, which was not enough time to generate that many logs. The query timeout has been increased to 60 minutes as a fix.
69306	Fixed a misspelling displayed in the help details for the command <code>request quota-enforcement</code> in the Panorama command line interface (CLI).
69035	When using the ACC tab on the Panorama web interface to view statistics for a custom application, using applications filters (such as the Category, Subcategory, and Technology) to filter the displayed data resulted in no data being displayed. This occurred when Panorama was selected as the Data Source for the traffic data displayed on the ACC tab, and the issue has been resolved.
68982	Fixed an issue where the firewall stopped receiving new reports from WildFire™ when the report ID on the WildFire public cloud exceeded a certain limit (reports continued to be generated but were not logged on the firewall).
68899	Fixed an issue that affected PA-7050 firewalls. An issue occurred where an HSCI port configured as an HA2 interface went down due to a dataplane board restarting. An improvement has been made so that, if there are more than one dataplane boards up and running, a single dataplane restart will not cause an HA2 interface on an HSCI port to go down.
68885	Fixed an issue that occurred after upgrading Panorama. Administrators that did not have local access, but that were previously authenticated to Panorama, could not log in to the CLI and an error message was displayed.
68836	In a high availability (HA) setup, a path monitoring failure lead to a delayed HA failover. An update has been made to optimize HA failover time.
68768	A base OVF image is available for PAN-OS 6.1. To find the new image, filter by Pan-OS for VMware NSX Base Images on the Palo Alto Networks Support Portal .
68702	An error was displayed when pushing a policy from Panorama to a managed firewall with a user group defined in the policy. The error displayed was <code>Duplicate group name</code> and this issue has been resolved so that pushing a user group from Panorama to a managed firewall works correctly.

Issue Identifier	Issue Description
68588	Predefined reports for a firewall connected to Panorama were not being displayed correctly if the management server for the firewall was not restarted after connecting to Panorama. This issue has been fixed so that predefined reports from a managed firewall are still displayed correctly after establishing a connection with Panorama.
68528	Modifying a policy rule by removing a Source User entry and using the Any default for the Source User field resulted in a commit failure when attempting to save the changes. This issue has been fixed so that when a source user is removed from a policy rule, the policy rule can be successfully modified to use the default of Any .
68498	Fixed an issue where a validation error occurred when pushing a service from Panorama to a managed firewall.
68491	Certificates expiring after the year 2050 showed an error for the certificates' validity time field. This was due to an issue where, when decryption was performed on a certificate, the standard field meant to display when the certificate expires (<code>generalizedTime</code>) was modified to display a field that is not standard (<code>utcTime</code>). This has been updated so that the validity for a certificate expiring after the year 2050 is displayed correctly.
68472	Addressed an issue where some expected counters were not returned in the output for the XML API command <code><show> <interface></code> for loopback, VLAN, and tunnel interfaces.
68409	When setting up BGP Import Rules or Export Rules , configuring a Community Type as Append and then an Append value of <code>AS:0</code> displayed an error (Network > Virtual Routers > BGP > Import/Export > Action > Community). This issue has been fixed to allow the value of the Append field to be <code>AS:0</code> or <code>0:N</code> (<code>0:0</code> as a value is not supported).
68389	The Application sub-category is listed as unknown in the PDF report for custom applications pushed from Panorama. This issue was resolved by correcting the report daemon to properly parse the configuration objects pushed from Panorama.
68380	An issue occurred when a device group configuration was pushed from Panorama to a managed device. When the commit failed, neither the Panorama web interface nor the CLI displayed an error message. The web interface continued to display the status <code>config sent to device</code> and the CLI showed the failures status of the jobs; however, neither the web interface nor the CLI displayed an error message. A fix was made to display commit errors and details for Panorama and the managed device that did not correctly receive the pushed configuration.
68372	Setting up a static MAC configuration for a tagged interface configured on a VLAN did not work correctly. This was due to an issue where a process that communicates between the dataplane and the management plane restarted, and the issue has been resolved.
68371	Addressed an issue where you could not install the BrightCloud database when the default url-db was set to PAN url-DB, and you had not downloaded the BrightCloud database previously.

Issue Identifier	Issue Description
68355	For a device in a high availability (HA) active/active configuration, the web interface displayed an incomplete list of the HA virtual addresses configured to be used in the HA active/active cluster—the Virtual Address table displayed only six interfaces with assigned IP addresses when eight interfaces were actually configured. A scroll bar has been added to the Virtual Address table to allow you to scroll up or down to view the complete list of configured HA virtual addresses (Devices > High Availability > Active/Active Config > Virtual Address).
68320	The Logging and Reporting Settings section on the web interface incorrectly displayed a logarithm for unallocated Log Storage when the total allocated log storage quota was configured to be 100% and unallocated log storage was 0% (Device > Setup > Management). This was a cosmetic issue and has been fixed so that Log Storage on the Logging and Reporting Settings window displays unallocated log storage as 0 MB when log storage is 100% allocated.
68319	When FIPS mode was enabled, the web interface becomes unresponsive when configuring a GlobalProtect gateway and a browser refresh was required to continue using the web interface. A check was introduced to ensure that the web interface does not become unresponsive when creating a GlobalProtect gateway with FIPS mode enabled.
68286	An issue was seen where setting up a password for a proxy server caused the management plane to restart (Device > Setup > Services > Proxy Server). This was due to a back-end process restarting when the password was configured and has been fixed.
68100	An issue was resolved where the Strip X-Forwarded-For Header option did not correctly remove an internal IP address (Device > Setup > Content-ID).
68055	Mac clients were incorrectly unable to access certain websites that Windows clients were able to access. This issue occurred when fragmented traffic passed through the firewall and the first fragment did not include the header; this caused packets to be dropped. The issue has been resolved.
67864	When a rule pushed from Panorama is selected on a managed device, the Clone button in a security policy is enabled; however, rules pushed to a managed device from Panorama cannot be cloned on a managed device. With this fix, the Clone button for rules pushed from Panorama correctly shows as disabled on the web interface for a managed device.
67810	When a PA-5000 Series device initiates sessions on different data planes in an environment with multiple virtual systems, sometimes session traffic failed to span across virtual systems. This issue has been resolved so that inter-virtual system sessions succeed with a dynamic network address translation (NAT) policy configuration.
67676	Upgrading Panorama to a major release resulted in Panorama losing connectivity with managed firewalls (a major release is any release where the release number ends in 0, for example PAN-OS 6.0.0 or PAN-OS 6.1.0). This was due to an issue with the log schema file and an update was made to ensure that the log schema file is overwritten during an upgrade, even if the file size is zero.
67567	When a new version of the BrightCloud URL database was downloaded and installed, if there was a change to the category for a URL between the old and the new database, the change was not reflected on the dataplane. With this fix, URL categories on the dataplane are updated correctly after installing a new version of the BrightCloud database.

Issue Identifier	Issue Description
67516	Fixed an issue with a high availability (HA) active/active configuration where a physical MAC address was returned for a floating IP address instead of a virtual MAC address. This has been addressed so that the floating IP correctly responds to ARP requests with a virtual MAC address.
67455	Made an update to the enforcement for the SSL Inbound Inspection setting block when resources are unavailable so that hosts cannot resume an SSL session, when that session has been removed from the SSL-decrypt session cache due to the cache being full. The host must start a new session to continue.
67436	The commands <code>debug software trace reportd</code> and <code>debug software core reportd</code> were added to the CLI command structure.
67344	Fixed an issue for the M-100 appliance where the <code>show log-collector detail</code> command was presenting incorrect information.
67300	Addressed an issue on the VM-Series firewalls where enabling packet capture for certain application-level gateway (ALG) traffic caused the system to restart.
67258	The process (<i>mprelay</i>) that communicates between the dataplane and the management plane restarted unexpectedly. A policy-based forwarding (PBF) rule configured with symmetric return but not specifying an IPv6 next hop address resulted in excessive neighbor discovery (ND) update messages that caused a conditional loop, which then caused the <i>mprelay</i> process to restart. With this fix, the IPv6 ND performs correctly and avoids unexpected restarts of the <i>mprelay</i> process even if no IPv6 next hop address is specified.
67187	The following error was displayed due to an issue that caused a User-ID process to restart: <code>Abnormal system memory usage detected, restarting userid with virtual memory</code> . Many GlobalProtect users logging into the system, and the resulting high availability (HA) synchronization of the HIP reports, caused the virtual memory to exceed its limit.
66953	The maximum number of tags that PAN-OS and Panorama support for each virtual system and device group (including the Shared group) is now 2,500 instead of 1,000.
66920	Secure Shell (SSH) traffic was incorrectly categorized as URL Category <code>unknown</code> . This has been fixed so SSH traffic is not assigned a URL category.
66630	After changing the domain name setting in an LDAP server profile, users failed to authenticate with the new LDAP server. This was due to a missing function that updates the internal group database name and has been resolved.
66466	Addressed an issue for the PA-2000 platform, where a device failed to handle high volume of packets (larger than the MTU) on the management interface. Symptoms of this issue included device unresponsiveness, a random restart, traffic failures or ATA errors on the console. This issue has been resolved.
66364	Fixed an issue that prevented two certificates with the same subject name from being installed following an upgrade to PAN-OS 6.0.X.
66220	An issue was seen in a high availability (HA) active/passive configuration where the secondary device was not able to pass traffic after a failover until a routing process was restarted. This issue has been fixed so that when a failover occurs, the secondary device correctly becomes the Backup Designated Router (BDR).

Issue Identifier	Issue Description
66073	An issue with the command <code>debug system ssh-key-reset high-availability</code> generating a 0 byte key file has been resolved. This issue has been resolved so that the <code>debug system ssh-key-reset high-availability</code> command generates valid key files.
66010	The firewall did not resolve FQDNs used in policies when the DNS responses contained Canonical Names (CNAMEs) with capital letters. With this fix, the firewall properly resolves the FQDNs, regardless of the case of the letters in the returned CNAMEs.
65859	Fixed an issue where the dataplane could restart when SSL Forward Proxy decryption was enabled and a certain packet sequence was received.
65850	Addressed an issue where a high availability (HA) backup failed due to there being no buffer space available.
65565	Fixed an issue where selecting Replay attack detection in the GlobalProtect gateway satellite configuration did not actually enable replay attack detection when configured in the web interface.
64930	Dynamic objects could be lost if the device server restarted unexpectedly. This has been fixed so that dynamic objects are repopulated if the device server process unexpectedly restarts.
63150	In a high availability (HA) active/active configuration, User Datagram Protocol (UDP) sessions with a certain traffic pattern caused the session state to flap frequently and generate excessive traffic logs. This issue is now fixed and the session state is stable.
62768	Unreliable DNS servers incorrectly provide NXDOMAIN responses. To help prevent incorrect WildFire sample categorization, NXDOMAIN responses are no longer shared across WildFire samples. Each NXDOMAIN response will be evaluated on a sample by sample basis.
61205	Using the web interface to export traffic logs in CSV format was showing an error that the query job failed. This issue has been addressed so that exporting traffic logs to CSV works correctly.

PAN-OS 6.1.0 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 6.1.0 release. For new features, associated software versions, known issues, and changes in default behavior, see [PAN-OS 6.1 Release Information](#). Before you upgrade or downgrade to this release, review information about how to [Upgrade to PAN-OS 6.1](#).



If you have asymmetric routes in your network, before [upgrading to 6.1.0](#), use the following command to ensure session continuity: `set deviceconfig setting tcp asymmetric-path bypass`. And, if you have attached a zone protection profile, you must also use the following command: `set network profiles zone-protection-profile <profile-name> asymmetric-path [bypass | global]`.

Issue Identifier	Issue Description
69173	Under certain conditions, unspecified layering of packet-level evasions could be used to bypass signature matching of the session.
68708	Addressed the bash vulnerability CVE-2014-7169 that relates to how environment variables are processed when the shell starts up. This fix prevents a user with an account on the firewall, from using the vulnerability to gain escalated privileges.
67833	While generating a tech support file on Panorama, private information was not being removed correctly from files within a device group if the device group had a space in its name. With this fix, device groups with spaces in their names are handled correctly when generating a tech support file.
67814	Panorama displayed the secure-proxy-password in the web interface under Panorama > Setup > Services and in the CLI. With this fix, Panorama encrypts the secure-proxy-password and downgrade attempts to versions which show the secure-proxy-password will fail until you remove the secure-proxy-password from the configuration.
67788	The configuration log on Panorama displayed the secure-proxy-password. With this fix, the configuration log encrypts the secure-proxy-password.
67782	If a policy had more than one tag, and you wanted to filter the policies based on one tag but not the other tag, the logic failed and the filter did not work. With this fix, the filter is working as expected.
67720	The Network Processing Card (NPC) on the PA-7050 firewall continually restarted when link errors were present, causing a system restart to occur. An update to the internal link failure recovery logic now prevents system restarts when link errors are present.
67674	Resolved an issue where a misspelling in a label in the PAN-TRAPS.my MIB file resulted in a failure to load the MIB.
67268	When configuring DNS sinkhole, the firewall was unable to display the IP address of the client that was initiating corrupt DNS requests in the logs. With this fix, the logs display the source IP address of the client.

Issue Identifier	Issue Description
67182	External Block Lists (EBLs) were not properly parsed during the initial load. This caused the load to fail if Windows formatted files were used, where <CR><LF> line feeds were used instead of standard UNIX <LF>. Comments were also not properly supported on the same line as the IP, IP-RANGE, and IP-MASK. After fixing the issues, both types of line feeds and comments are now supported.
66953	The maximum number of tags that PAN-OS and Panorama support for each virtual system and device group (including the Shared group) is now 2,500 instead of 1,000.
66924	When logging in to the Panorama web interface with two-factor RADIUS authentication, Panorama would successfully authenticate the user but then immediately log the user out of the web interface. With this fix, Panorama no longer logs the user out of the web interface following a successful authentication.
66918	Memory corruption issues related to SSL decryption caused the data plane to restart and resulted in a flapping condition between firewalls in an HA cluster.
66862	If the certificate name length had more than 31 characters and it was used in a decryption policy for SSL inbound inspection, a commit would fail. With this fix, validation fails when the certificate used in an SSL inbound inspection decryption policy has more than 31 characters inside the certificate name field.
66826	Due to SSL errors caused by the way the serial number is generated in the device certificate, you could not manage multiple WF-500 WildFire™ appliances from the same browser.
66761	To accommodate large quantities of scheduled reports with long reporting periods, the M-100 appliance now supports increased storage capacity.
66711	The passive device in a HA cluster triggers DOS alerts about a session limit reached for a classified DOS profile. After the fix, the passive device no longer receives the DOS logs since it is not processing any traffic.
66701	You can now increase the capacity of the Address Resolution Protocol (ARP) table and the MAC address table on PA-3020 and PA-3050 devices using the <code>debug system arp-mac-capacity increased</code> command. On the PA-3020 platform, running this command increases the maximum number of table entries from 1500 to 3000. On the PA-3050 platform, running this command increases the maximum number of table entries from 2500 to 5000.
66693	When a Port Address Translation (PAT) rule was configured to only change the destination port but not IP address for that host, Address Resolution Protocol (ARP) was not learned from a destination host on a connected network. With this fix, ARP resolves correctly.
66635	Enabling SSL Forward Proxy decryption with a self-signed certificate could sometimes cause the certificate presented to the client to have a negative serial number.
66520	An update has been made so that when you commit with an IP address/Netmask configured but do not select an HA port in HA settings, PAN-OS shows additional details on the commit fail error message that indicate the specific incomplete HA settings.
66482	In some cases you could not access the web interface for an M-100 appliance even though you could access the appliance through the CLI. The issue is now addressed so that you can access both the web interface and the CLI on an M-100 appliance.

Issue Identifier	Issue Description
66372	Fixed an issue where some threat names did not display correctly in threat logs forwarded from the firewall when the logs were viewed on a syslog server.
66360	Fixed an issue on the Panorama web interface, where hovering the mouse over the High Availability widget on the Dashboard was displaying incorrect information for threat versions.
66358	When a copper small form-factor pluggable (SFP) link speed was forced to 1000 Mbits/s, the interface state remained up even if there was no network cable attached. With the fix, the interface state now reflects the actual state of the network connectivity.
66208	A brute-force attack on an unprotected management interface on the firewall caused the <code>/var/log/btmp</code> log file to inflate and consume available disk space. With this fix, PAN-OS enables a log rotation function for failed SSH logins, such as those from brute-force attacks.
66021	After a client certificate was revoked, the GlobalProtect™ portal allowed users to log in one more time. After resolving this issue, GlobalProtect blocks all login attempts after revoking the client certificate.
66005	Previously, <code>show_log_system.txt</code> in the techsupport file contained 50,000 lines showing the oldest events and did not display the latest events if <code>show log system</code> had more than 50,000 lines in the system. The logs now display the recent events first.
66002	An issue with the Host Information Profile (HIP) report caused firewalls running PAN-OS to retain host information even after a GlobalProtect user logged out. In this case, the same client IP address was assigned to another user due to the HIP match and the traffic was handled according to the security policy that applied to the previous user.
65922	Improvements have been made to session management for PA-5000 platform devices.
65909	When configuring an HIP profile to check two drives for disk encryption, evaluation fails although the HIP report is correct. After the fix, the evaluation succeeds when configuring the HIP profile to check for two drives.
65866	Using the web interface, you can now configure the option to discard embedded ICMP error packets in the zone protection profile. Previously, you could only configure this option using the CLI.
65721	When pushing Wi-Fi settings to Android mobile devices, GlobalProtect did not set security parameters when an SSID was hidden, and prompted users to authenticate when the SSID was visible. With this fix, GlobalProtect correctly pushes the Wi-Fi settings to Android mobile devices.
65302	On the Panorama web interface, filtering security policies to display the policies for a specific device group displayed shared policies that were not targeted to any device in that device group. With this fix, the Panorama web interface only shows shared policies that are targeted to a device in the selected device group.
65294	In syslog and <code>devsrv.log</code> output, a message about the last known update from the PAN-DB cloud was labeled as seconds instead of minutes. The description of the log pattern now displays the correct label.

Issue Identifier	Issue Description
65220	With SSH proxy enabled, traffic to some SSH servers failed. With this fix, traffic to the SSH servers no longer fails when SSH proxy is enabled.
65174	Resolved an issue where an <code>Invalid IP Address</code> error was shown when creating a redistribution profile from within the Export Rules in OSPF or Redistribution Rules in BGP.
65031	During a high availability (HA) active/passive failover, a timing issue delayed the reestablishment of end-to-end connectivity for OSPF interfaces. The graceful restart hello delay timer now allows you to configure the length of time during which the firewall sends grace LSA packets. From the CLI, use the <code>gr-delay</code> option to specify the graceful restart delay on OSPF interfaces.
64759	Fixed an issue where a high availability (HA) failover occurred due to insufficient kernel memory on a PA-5000 Series firewall that was attempting to handle unusually heavy network and system traffic. With this fix, the kernel memory on PA-5000 Series firewalls is increased to ensure sufficient kernel memory is available for ping requests and keep-alive messages even when under an unusually heavy load.
64751	Addressed an issue where SNMPv3 traps sent from the firewall for the EngineBoots and EngineTime variables were incorrectly set in the SNMP header.
64713	Removed support for the RC4-MD5 and RC4-SHA cipher suites. These ciphers cannot be used to negotiate an SSL/TLS connection to the GlobalProtect portal or to the management interface of the firewall.
64606	When navigating to the GlobalProtect portal using a browser that had Transport Layer Security (TLS) 1.2 enabled, and when using a client certificate for authentication, the SSL connection failed due to issues with the fallback to a lower TLS version. With this fix, the fallback succeeds with Google Chrome and Mozilla Firefox. This specific behavior of Internet Explorer still exhibits issues.
64600	When a dynamic block list was configured on the firewall to be updated according to a list on a configured proxy server, the firewall was unable to access the proxy server. This issue has been resolved so that the firewall can correctly access the list on the proxy server to update the dynamic block list.
64439	When you configured QoS on an interface that was saturated with traffic from QoS classes without bandwidth guarantees, traffic from QoS classes with guaranteed bandwidth experienced traffic loss. This was due to rounding errors, which caused the total calculated interface bandwidth to exceed the actual bandwidth. With this fix, the bandwidth limits are properly calculated and no traffic loss is observed.
64389	In certain situations, when performing an HA failover, GlobalProtect clients connecting to the gateway using IPsec were disconnected and did not reconnect after the failover of the gateway. This issue has been fixed, and the GlobalProtect client reconnects to the new active gateway.
64310	When performing an application dump (to capture packets for a particular application) for a specific security rule, an application dump was performed for all security rules. This issue has been fixed so that specifying a security rule for an application dump only performs an application dump for traffic matching that rule.

Issue Identifier	Issue Description
64279	An enhancement has been made to lower the configurable amount of time at which the firewall refreshes FQDN object entries. The previous lowest amount of time you could configure for FQDN refreshes to occur was every 1800 seconds. You can now use the <code>fqdn-refresh-time</code> command to configure FQDN refreshes to occur every 600 seconds – 14,399 seconds.
64229	A QoS policy was not being enforced on the firewall and all traffic was being classified and treated as class 4 traffic (the default QoS class). This issue has been resolved so that a configured QoS policy is correctly enforced on traffic.
64223	Fixed an issue where FQDN objects that were added to a dynamic address group were not listed after issuing the command <code>request system fqdn show</code> , with the command displaying a message that no FQDN object is used in the policies.
64040	Addressed an issue where a log collector's disk usage exceeded the total log storage quota configured on Panorama (Templates > Panorama > Collector Groups > Log Storage Settings).
63857	In certain circumstances, an application could have been implicitly allowed through the firewall due to a configured rule that allowed only a dependent application. The issue has been fixed so that an application that might be implicitly allowed is properly blocked if needed.
63790	A firewall that did not have a GlobalProtect license and was configured with one portal and one gateway was displaying a commit warning when the cutoff time for a GlobalProtect gateway was set to any other value than the default value of 5 seconds (the cutoff time is how long a GlobalProtect agent will wait for the GlobalProtect gateways to respond in determining the best gateway to connect to). This issue has been fixed so that a commit warning is not displayed when the cutoff time for a GlobalProtect gateway is set to a value other than the default.
63641	When an LDAP authentication profile was configured with the Password Expiry Warning set to the default of 7 days, a warning message was not shown 7 days before the password was set to expire. This issue has been fixed so that users are correctly warned before their passwords expire, depending on the number of days entered in the Password Expiry Warning field.
63349	Fixed an issue where Dynamic Host Configuration Protocol (DHCP) leases were being reset when the firewall was restarted.
63218	The web interface allowed for a security policy to be created with the Service defined both as application-default and a specific service. This has been fixed so that you can either select the application-default option so that selected applications are either allowed or denied on their default ports or select a specific service or service group to limit to specific TCP/UDP port numbers (you cannot enable both of these options within a single security policy).
63123	The CLI command <code>test security-policy-match</code> with the <code>show-all</code> flag does not list all policies that match the defined criteria. The algorithm starts at the top of the rulebase and checks all rules until it finds the first rule that matches the defined criteria. The algorithm does not continue to check subsequent rules after this match occurs. Because this command only displays a list of potential matches and is not an exhaustive list, the explanatory text has been updated to reflect this behavior.

Issue Identifier	Issue Description
63010	An issue was seen while uploading large files to the WildFire cloud, where the firewall received an error that the file size exceeded the limit. As a result, the cloud connection continued to reset, blocking all other files in the upload queue. With this fix, files that exceed the limit to upload to the cloud are dropped and next file continues to be processed.
62791	An update was made to reduce the number of TCP stale sessions for PA-5000 series devices.
62644	When a copper SFP port was plugged in, the SFP interface's link displayed unknown/unknown/up; this has been updated to more accurately display auto/auto/up.
62222	Fixed an issue where a malicious DNS lookup did not generate a threat log when an anti-spyware profile was defined to allow low severity spyware.
62146	An update was made so that the firewall sends the NetFlow/IPFIX private enterprise number field value as a 32-bit number. It was previously sending the private enterprise number field value as a 16-bit number.
62018	The RADIUS Server Profile dialog indicated an error if you entered more than 15 characters for the Secret value, even though the character limit is 64. The dialog no longer displays an error as long as you enter no more than 64 characters.
61631	Fixed an issue that occurred when HA control packets were routed through the dataplane, causing OSPF neighbors to continually flap.
61489	Attempting to generate an certificate on Panorama using the CLI displayed the following error: <code>Internal error. Failed to insert xml node.</code> You can now generate certificates correctly for Panorama using the CLI.
61328	The restart speed has been optimized for Panorama when using NFS logs storage. This includes removing an unnecessary scanning of the threat log directory that was leading to a long start-up process.
61186	When managing multiple log collectors with Panorama, changing the name of a log collector group or deleting a log collector group caused a loss of logs. To prevent this, you can no longer change the name of an existing log collector group. Additionally, a warning is now displayed when attempting to delete a log collector group.
60893	A Java applet was incorrectly classified as malware by WildFire. This was due to an issue where the applet attempted to read a username, which requires permission from the Java virtual machine. The specific Java applet that was incorrectly classified has been reviewed and identified as a benign file.
60710	The CLI command <code>request certificate generate</code> failed to generate a certificate on Panorama. The command now generates a certificate as expected.
60341	Fixed an issue where renewing a server certificate was only effective for GlobalProtect portals and gateways by restarting the firewall. This issue has been fixed so that renewing server certificates for GlobalProtect portals and gateways works correctly without restarting the firewall.
60042	Fixed an issue where applying filters to search for or view security policies was not correctly displaying all the policies that matched the filter.

Issue Identifier	Issue Description
60022	Resolved an issue where for Session Initiation Protocol (SIP) traffic from a mobile device, a policy-based forwarding rule was only being applied to the client to server traffic flow, and not to the server to client traffic flow for the same session.
59304	Fixed an issue where User-ID lost group mapping information following an OpenLDAP refresh. This was due to the OpenLDAP server allowing the same name to be used as an object name and a user account and has been resolved.
58547	Policy-based forwarding (PBF) with symmetric return did not work when the traffic was translated with source NAT. Return traffic, which needs to be forwarded via the same interface on which it arrived, was dropped with the message <code>Symmetric Return: Packet dropped, no return MAC found</code> . The issue is fixed.
57917	Some tables in a firewall PDF summary report did not display correctly. Fixed an issue where no line was displayed between two points in a line graph, and another issue where the Top 5 Applications table was not correctly sorted to display the applications in descending order.
56452	Fixed an issue where you could not configure subinterfaces with VLAN tags (divide a physical interface into multiple logical interfaces that filter traffic based on VLAN tags) on the VM-Series firewall on a Citrix SDX server unless you disabled VLAN stripping on 1-gigabit ports assigned to the VM-Series firewall.
55370	With SSH proxy configured, if the SSH client performed a key renegotiation, the client would be disconnected and an error would be displayed that the server's host key did not match the signature supplied. An update was made to allow the new key to be accepted.
55249	You can now run the CLI command <code>test <feature></code> for the following features: <code>botnet, cp-policy-match, custom-url, data-filtering, decryption-policy-match, dns-proxy, dos-policy-match, global-protect-mdm, global-protect-satellite, nat-policy-match, nd, pbf-policy-match, pppoe, qos-policy-match, routing, scp-server-connection, security-policy-match, stats-service, tag-filter, url, url-info-cloud, url-info-host, user-id, vpn, wildfire</code> .
54483	Resolved an issue where a fragmented DHCP response could cause packet processing services on the dataplane to restart.
33211	If the running configuration had more than 16,777,215 lines, the CLI command <code>show config running</code> failed to display the configuration: it displayed an out of range error. This has been fixed so that <code>show config running</code> displays the configuration regardless of size.



Getting Help

The following topics provide information on where to find out more about our products and how to request support:

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

Related Documentation

Refer to the following documents on the Technical Documentation portal at <https://www.paloaltonetworks.com/documentation> for more information on our products:

- [New Features Guide](#)—Detailed information on configuring the features introduced in this release.
- [PAN-OS Administrator's Guide](#)—Provides the concepts and solutions to get the most out of your Palo Alto Networks next-generation firewalls. This includes taking you through the initial configuration and basic set-up on your Palo Alto Networks firewalls.
- [Panorama Administrator's Guide](#)—Provides the basic framework to quickly set up the Panorama virtual appliance or the M-100 appliance for centralized administration of the Palo Alto Networks firewalls.
- [WildFire Administrator's Guide](#)—Provides information on deploying, operating, and maintaining the WildFire cloud and the WildFire WF-500 appliance and the Palo Alto Networks firewalls.
- [VM-Series Deployment Guide](#)—Provides details on deploying and licensing the VM-Series firewall on all supported hypervisors. It includes example of supported topologies on each hypervisor.
- [GlobalProtect Administrator's Guide](#)—Takes you through the configuration and maintenance of your GlobalProtect infrastructure.
- [Online Help System](#)—Detailed, context-sensitive help system integrated with the firewall web interface.
- Open Source Software (OSS) Listings—OSS licenses used with Palo Alto Networks products and software:
 - [PAN-OS 6.1](#)
 - [Panorama 6.1](#)
 - [WildFire 6.1](#)

Requesting Support

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

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

Contact Information

Corporate Headquarters:

Palo Alto Networks
4401 Great America Parkway
Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2014–2017 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

Revision Date: April 28, 2017