PAN-OS® 6.0.15 Release Notes

Revision Date: November 16, 2016

Review important information about Palo Alto Networks PAN-OS 6.0 software, including new features introduced in this release, workarounds for open issues, and resolved issues. For the latest version of this release note, refer to the Palo Alto Networks Technical Documentation portal.

PAN-OS 6.0 Release Information

This release note provides important information about Palo Alto Networks® PAN-OS® 6.0 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 6.0 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 6.0 Release Notes on the Technical Documentation portal.

- Features Introduced in PAN-OS 6.0
- Changes to Default Behavior
- Associated Software Versions

> Starting with PAN-OS 6.0.15, 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 6.0.15 Addressed Issues
- PAN-OS 6.0.14 Addressed Issues
- PAN-OS 6.0.13 Addressed Issues
- PAN-OS 6.0.12 Addressed Issues
- PAN-OS 6.0.11 Addressed Issues
- PAN-OS 6.0.10 Addressed Issues
- PAN-OS 6.0.9 Addressed Issues
- PAN-OS 6.0.8 Addressed Issues
- PAN-OS 6.0.7 Addressed Issues
- PAN-OS 6.0.6 Addressed Issues
- PAN-OS 6.0.5-h3 Addressed Issues
- PAN-OS 6.0.5 Addressed Issues
- PAN-OS 6.0.4 Addressed Issues
- PAN-OS 6.0.3 Addressed Issues
- PAN-OS 6.0.2 Addressed Issues
- PAN-OS 6.0.1 Addressed Issues
- PAN-OS 6.0.0 Addressed Issues
- Getting Help

Features Introduced in PAN-OS 6.0

The following topics describe the new features introduced in the PAN-OS 6.0 release. This release requires content version 401 or later. For details on how to use the new features, refer to the New Features Guide.

- ▲ App-ID
- ▲ Content Inspection Features
- ▲ GlobalProtect Features
- ▲ Management Features
- ▲ Networking Features
- ▲ Panorama Features
- ▲ User-ID Features
- ▲ Virtualization Features

App-ID

The following App-ID™ features are introduced in PAN-OS 6.0. For more details about these features and for instructions on configuring them, refer to Application Identification Features in the New Features Guide:

New Application Identification Feature	Description
Support for Hardware Security Modules	You can now offload the certificate signing functions for SSL forward proxy, SSL inbound inspection, and the master key storage functions to a dedicated hardware security module (HSM) for enhanced key management security. This release supports the use of the following HSMs: SafeNet Network and Thales nShield Connect. HSM support is generally required when FIPS 140-2 Level 3 protection for CA keys is required. The use of an HSM is supported on PA-7050, PA-3000 Series, PA-4000 Series, PA-5000 Series firewalls, VM-Series firewalls (VM 100, VM-200, VM-300, and VM-1000), and on the M-100 appliance. To configure a firewall to operate with an HSM, navigate to **Device > Setup > HSM**.
Option to Disable SIP ALG	By default, a Session Initiation Protocol (SIP) application-level gateway (ALG) performs NAT on the payload and opens dynamic pinholes for media ports. However, some SIP endpoints have NAT intelligence embedded in their clients. Because the firewall must not modify the signaling sessions in this case, you can now disable the SIP ALG functionality depending on the SIP applications in use in your environment. When SIP ALG is disabled, if App-ID determines that a session is SIP, the payload is not translated and open dynamic pinholes are not opened. To disable the SIP ALG, navigate to **Objects > Applications** and then customize the **ALG** option on the SIP application.

Content Inspection Features

The following Content Inspection features are introduced in PAN-OS 6.0. For more details about these features and for instructions on configuring them, refer to Content Inspection Features in the New Features Guide:

New Content Inspection Feature	Description
DNS Sinkholing	This feature adds a new sinkhole action to the DNS signatures within the Anti-Spyware profile. Sinkholing enables the firewall to forge a response to a DNS query for a known malicious domain, causing the malicious domain name to resolve to an IP address that you define. You can use this feature to identify infected hosts on the protected network using DNS traffic in situations where the firewall cannot see the infected client's DNS query (for example, when the firewall is north of the local DNS server). This feature can also be used to redirect malicious traffic to a honeypot or any other target host. Enable sinkholing for the DNS signature collection by selecting the **sinkhole** action in the **DNS Signatures** tab of an Anti-Spyware profile and specifying an IPv4 and/or IPv6 address to use as the sinkhole (the default is the localhost, which will cut off communication). The sinkhole address can be an address of a live server or an unused address on your network. After enabling DNS sinkholing, you can identify infected clients by filtering the traffic logs or by building a custom report that checks for sessions to the IP address you defined as the sinkhole address.
Extended Packet Capture	A new extended-capture option has been added to Anti-Spyware and Vulnerability Protection profiles for rules and exceptions defined in the profile. Previously, when selecting packet capture, only the first trigger packet would be captured when a threat was detected in traffic matching the profiles. With the extended-capture option enabled, the firewall can capture from 1 to 50 packets, which provides much more context when analyzing the threat logs. To define the number of packets to capture, navigate to **Device > Setup > Content-ID** and then edit the Threat Detection Settings section. You can then view the extended packet captures from the threat logs (**Monitor > Logs > Threat**) by locating the log entry you want to investigate and then clicking the green arrow (Packet Capture) icon in the second column.
Passive DNS	This is an opt-in feature that enables the firewall to act as a passive DNS sensor and send select DNS information to Palo Alto Networks for analysis to improve threat intelligence and threat prevention capabilities. The data collected includes non-recursive DNS query and response packet payloads (such as payloads originating from the local recursive resolver, not individual clients). This information is used by the Palo Alto Networks threat research team to gain insight into malware propagation and evasion techniques that abuse the DNS system. Information gathered through this data collection is used to improve accuracy and malware detection abilities within PAN-DB URL filtering, DNS-based command-and-control signatures, and the WildFire™ security service. Passive DNS monitoring is disabled by default but it is recommended that you enable it to facilitate enhanced threat intelligence. To enable this option select the **Enable Passive DNS Monitoring** check box on the **DNS Signatures** tab of the Anti-Spyware profile dialog for the Anti-Spyware profile that is attached to the security policy governing your DNS server's external DNS traffic.
URL Filtering Search Engine Cached Site Enhancement	An enhancement has been made to the URL filtering engine such that URL filtering policies will also be applied when end-users attempt to view the Google and Internet Archive cached copies of websites.

New Content Inspection Feature	Description
URL Filtering Translation Site Filtering Enhancement	An enhancement has been made to the URL filtering engine such that URL filtering policies will also be applied to any URLs that are entered into translation sites such as Google Translate. This will ensure that website translation tools are not used to bypass URL filtering policies.
URL Filtering Safe Search Enforcement	This feature prevents users from viewing the search results unless the strictest safe search option is set in their browsers for and when searching using one of the top three search providers (Google, Bing, and Yahoo). If the strictest safe search option is not set in the browser, users will see a block page instructing them how to set the option for the given search provider. To enable this option, select the **Safe Search Enforcement** check box in the URL Filtering profile. Safe search will then be enforced whenever a user request matches a security policy rule with the corresponding URL Filtering profile attached. Starting in PAN-OS 6.0.1, YouTube Safety Mode is supported as part of URL Filtering Safe Search Enforcement. YouTube Safety Mode ensures that YouTube search results only appear when the strictest safe search option is set in the user's browser. Additionally, Safe Search Enforcement support for the Yandex search engine was added in content release version 446. Finally, transparent safe search enforcement is supported with content release version 475 or later.
WildFire Report Incorrect Verdict Option	When viewing a WildFire analysis report for a sample that has been analyzed by WildFire, a new feature called **Report Incorrect Verdict** is now available in the report. This option enables you to resubmit the sample to the Palo Alto Networks threat team if you feel the verdict is a false positive or false negative. The threat team will perform further analysis on the sample to determine if it should be reclassified. If a file that was previously identified as malicious is determined to be benign (false positive), the signature for the file will be disabled in an upcoming antivirus signature update. Similarly if a file that was previously identified as benign is determined to be malicious (false negative), a new signature will be generated and distributed in the next content update. After the investigation is complete, you will receive an email (if provided on the submission form) notifying you of the outcome.
WildFire Sandbox Operating Systems	Microsoft Windows 7 32/bit has been added to the WildFire environment. When a dynamic analysis is performed on a file, it will be run in Windows XP and Windows 7. On a WF-500 WildFire appliance, you will need to select an image that will contain Windows XP or Windows 7 as well as a combination of other applications, such as different versions of Adobe Reader, and MS Office.
Additional File Type Support Added to WildFire	As part of the WildFire subscription, the following advanced file types are now supported: Microsoft Office (.doc/.docx, .xls/.xlsx, and .ppt/.pptx); Portable Document Format (.pdf); Java Applet (.jar and .class); and Android Application Package (.apk). With a WildFire subscription, all listed file types can be submitted to WildFire from a PAN-OS firewall running PAN-OS 6.0 or later release versions using the WildFire web interface, a File Blocking profile in a security policy, or by manual upload to the WildFire portal at https://wildfire.paloaltonetworks.com. If you do not have a WildFire subscription, the firewall will forward only PE files. You can, however, manually upload any of the other supported file types to the WildFire portal. The WF-500 WildFire appliance does not support APK file analysis.

New Content Inspection Feature	Description
WildFire Analysis Report Enhancement	The WildFire analysis report is now integrated with the logging features of the firewall and no longer requires a WildFire subscription. In addition, several new enhancements have been made to the report, including the ability to: • Export the full report to a PDF by clicking **Download PDF**. • Download the file sample that was analyzed. • View the analysis results for each virtual environment in which the file was analyzed by clicking the corresponding **Virtual Machine** tab in the **Dynamic Analysis** section of the report. For example, click the **Virtual Machine 1** tab to view the Windows XP analysis results or click the **Virtual Machine 2** tab to see the analysis results for Windows 7. New virtual machine tabs will display as new environments are added. Each sandbox environment has its own configuration of applications and software used in the file analysis, such as which version of Adobe Reader, Flash, and MS Office are used in the file analysis on the specific virtual machine. • View all processes or filter by an individual process. • Re-submit the file sample to Palo Alto Networks for reevaluation if you think the file verdict (benign/malware) is incorrect by clicking **Report Incorrect Verdict**.
WildFire Logging Update	When a firewall is configured with a file blocking profile and security policy to forward files to WildFire for analysis, a WildFire subscription is no longer required to receive the WildFire Submissions logs on the firewall. A Subscription is still required to forward files to a WF-500 WildFire appliance and/or to forward the advanced file types that are now supported in PAN-OS 6.0 to either the WildFire cloud or a WildFire appliance.
WildFire Report Integration	Previously, in order to view the WildFire detailed report, you had to link to the report hosted on the WildFire cloud or the WildFire appliance. This report has now been integrated into the report on the firewall. Now, the WildFire Log Details report contains two tabs: • **Details** tab-Shows the session details. • **WildFire Analysis Report** tab-Shows the WildFire detailed report, which was previously hosted on the WildFire cloud or WildFire appliance. Panorama™ no longer requires all managed firewalls to forward files to the same WildFire system so long as Panorama and the managed firewalls are running a PAN-OS 6.0 or later release version.
WildFire Submissions Log Forwarding	Previously, you could only forward WildFire logs if you configured threat log forwarding for medium severity logs (which included WildFire logs with a malicious verdict) and/or informational severity logs (which included WildFire logs with a benign verdict). You can now configure the firewall to automatically forward WildFire Submissions logs independently of the threat log forwarding configuration. To enable WildFire Submissions log forwarding, configure the **WildFire Settings** in the log forwarding profile (**Objects > Log Forwarding**) to specify which WildFire logs (**Benign** and/or **Malicious** verdict) to forward to which log destinations (SNMP trap receiver, Panorama, syslog server, or email alert).
WildFire API Enhancements	The WildFire API syntax has changed for some web interface operations. For example, the file hash for sample files are now included in the logs, which you can use to query using the /get/report method. In addition, you can also now download WildFire PDF reports using the web interface and you can submit sample files to WildFire for the new files types that are now supported. For details on using the WildFire web interface in PAN-OS 6.0, refer to the WildFire Administrator's Guide.

GlobalProtect Features

The following GlobalProtect™ features are introduced in PAN-OS 6.0. For more details about these GlobalProtect features and for instructions on configuring them, refer to GlobalProtect Features in the New Features Guide.

New GlobalProtect Feature	Description
GlobalProtect Mobile Security Manager	Provides, management, visibility, and automated configuration deployment for the mobile devices-either company provisioned or employee owned-on your network. With Mobile Security Manager you can create user- and/or HIP-based deployment policies that allow you to push application configurations (such as email and VPN configurations) to your employees' mobile devices. The Mobile Security Manager requires the devices it manages to check-in regularly to ensure that the device is in compliance, pushing new configuration to devices if the device status changes (for example, if the Mobile Security Manager determines it has an app with malware installed) or to push an updated policy to the device. You can also perform certain actions on a managed device from the Mobile Security Manager, such as locking the device, sounding an alarm to help locate the device, or even wiping a device that has been compromised. In addition, the GlobalProtect gateways can retrieve extended HIP report information for the devices managed by the Mobile Security Manager and use the information to enforce security policies for devices that connect to your network. The Mobile Security Manager runs on the GP-100 appliance.
Agent Deployment Customization	All GlobalProtect agent customization settings can now be set in the Windows registry (`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`) or the Mac global plist file (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`). This enables deployment of GlobalProtect agent settings to client systems prior to their first connection to the GlobalProtect portal. For Windows clients, this also enables simplified deployment via group policy, as well as the option to automatically deploy the settings in the Windows Installer (MSIEXEC). Note that settings defined in the GlobalProtect portal client configuration take precedence over settings defined in the Windows Registry or the Mac plist. In addition, the following new configuration options have been added to the **Network > GlobalProtect > Portals Agent** tab in the **Configs** dialog: • **Show GlobalProtect icon**—Disabling this option makes GlobalProtect invisible to the end user by removing the icon from the system tray and preventing the user from having any interaction with the GlobalProtect agent user interface. • **Allow user to change portal address**—Disabling this option prevents users from manually changing the portal address pushed to the client in the portal configuration file. • **Allow user to continue if portal server certificate is invalid**—Disabling this option prevents users from continuing if there is a warning screen indicating a man-in-the-middle (MITM) attack,

New GlobalProtect Feature	Description
Transparent One-Time Password (OTP) Support	To simplify the GlobalProtect user authentication process and make it more transparent for the end user when authenticating to the portal and the gateway, the portal now includes settings for modifying the default authentication behavior on a per-client configuration basis. The following **Authentication Modifier** settings are now available on the **General** tab when configuring a client configuration on the portal (**Network > GlobalProtect > Portals**): • **Cookie authentication for config refresh**—Enables the agent to use an encrypted cookie to authenticate to the portal when refreshing a configuration that has already been cached (the user will always be required to authenticate to the portal for the initial configuration download and upon cookie expiration). This simplifies the authentication process for end users because they will no longer be required to log in to both the portal and the gateway in succession or enter multiple OTPs for authenticating to each. If this option is enabled, the portal will instead use the cookie to authenticate to the user. The cookie will never be used for authentication to the gateway. • **Different password for external gateway**—Disables the forwarding of credentials to some or all gateways, enabling the gateway to immediately prompt for its own set of credentials. This option speeds up the authentication process when the portal and the gateway require different credentials (either different OTPs or different login credentials entirely). Or, you can choose to use a different password on manual gateways only. With this option, the portal will forward credentials to automatic gateways but not to manual gateways, allowing you to have the same security on your portals and automatic gateways, while requiring a second factor OTP or a different password for access to those gateways that provide access to your most sensitive resources.
HIP Profile Support for Client DLP Products	The GlobalProtect agent by default now collects vendor-specific data about whether data loss prevention (DLP) software is installed and/or enabled on Windows hosts. DLP software is used to prevent sensitive corporate information from leaving the corporate network or from being stored on a potentially insecure device. Because this information is now collected from Windows host systems, you can include DLP as matching criteria for the host information profiles (HIPs) you create, thereby enabling you to use DLP compliance as criteria for your security policies.
Agent Update Control	The client configurations delivered by the GlobalProtect portal now have two additional options for controlling when users can upgrade the GlobalProtect agent: **disable** and **manual**. This means there are now four options for the **Agent Upgrade** field on the **Agent** tab in the Configs dialog of the portal configuration: • By default, the portal will **prompt** the agent to upgrade whenever a new version is available. • To enable automatic upgrades that do not require user interaction, select **transparent**. • (New option) To prevent agent upgrades, select **disable**. • (New option) To allow end users to initiate agent upgrades, select **manual**. In this case, the user would select the **Check Version** option in the agent to determine if there is a new agent version and then upgrade if desired.

New GlobalProtect Feature	Description
Certificate Authentication Enforcement	Enhancements have been made to how client certificate authentication is enforced in various scenarios as follows: • If a certificate profile is configured on the GlobalProtect portal, the client must present a certificate in order to connect. This means that certificates must be deployed to the end clients before their initial portal connection. • If the certificate profile specifies a **Username Field**, the certificate presented by the client must contain a username in order to connect. Furthermore, if both an authentication profile and a certificate profile with the **Username Field** are configured, the end user will be forced to use the username from the certificate to log in for authentication against the configured authentication profile. • For agents configured with the pre-logon connect method, if the new **Cookie authentication for config refresh** setting is enabled, you no longer need to configure a certificate profile for pre-logon authentication; in this case the portal will use the cookie to authenticate the client prior to user logon. Note, however, that you must still configure a certificate profile on the gateway to enable establishment of the VPN tunnel.

Management Features

The following Management features are introduced in PAN-OS 6.0. For more details about these features and for instructions on configuring them, refer to Management Features in the New Features Guide.

New Management Feature	Description
New Documentation Portal	The all new web-based Palo Alto Networks Technical Documentation portal is now available at https://www.paloaltonetworks.com/documentation.html. The new content you will find here features concepts and workflows that focus on enabling start-to-finish network security solutions. The documentation suite now covers the full Palo Alto Networks product and feature set, including the following new guides introduced in this release: • PAN-OS 6.0 New Features Guide • The new and improved PAN-OS Administrator's Guide • GlobalProtect Administrator's Guide • VM-Series Deployment Guide As of PAN-OS 6.0.4, this site has been enhanced so that all of the new workflow-based content is available in HTML with PDF downloads available on demand. This new format simplifies access to the documentation by allowing you to search for answers to specific questions, browse by product, or narrow the results by search facet. For details on how to get the most out of the new portal, watch the video.
Commit Improvement	The commit operation in Panorama and in PAN-OS has been enhanced to allow configuration edits during a commit. For example, if two administrators are logged in to the same firewall and the first administrator performs a commit, the second administrator can make updates to the configuration during the commit. This enhancement does not, however, allow multiple administrators to commit simultaneously.

New Management Feature	Description
Content Delivery Network (CDN)/Update Server Verification	Palo Alto Networks will begin transitioning to use of a CDN for delivery of software and content updates to devices running Panorama/PAN-OS 6.0 or later release version. This new process will provide a secure and distributed infrastructure to improve the software update process and license installation/verification for customers around the world. In addition, a new option has been added to strengthen all secure communication between firewalls/Panorama and the Palo Alto Networks update servers. To enable this option, select **Device** (or **Panorama**) **> Setup > Services** and select the **Verify Update Server Identity** check box in the **Services** dialog. When enabled, Panorama or PAN-OS will not perform a software/content download unless the update server has an SSL certificate signed by a trusted authority. This will help ensure that software updates and license verification will only be performed from Palo Alto Networks and will eliminate the possibility of man-in-the-middle attacks.
Enumeration of Rules within a Rulebase	The **Policies** tab on the web interface includes a new column for displaying rule numbers. Each rule is automatically numbered and the ordering adjusts as rules are moved or reordered. When filtering rules to find rules that match the specified filter(s), each rule is listed with its number in the context of the complete set of rules in the rulebase and its place in the evaluation order. In Panorama, pre-rules and post-rules are independently numbered. When rules are pushed from Panorama to a managed firewall, the rule numbering incorporates hierarchy in pre-rules, device rules, and post-rules within a rulebase and reflects the rule sequence and its evaluation order.
Enhancements in Reports	The reporting enhancements in this release include support for creating group activity reports and the ability to disable predefined reports. To generate reports for user groups on the firewall, select **Monitor > PDF Reports > User Activity Report**, select Type: **Group** and pick the group for which to generate the report. Because Panorama does not have the user to group mapping information, you cannot generate group activity reports on Panorama. To disable one or more predefined reports, select **Device** (or **Panorama**) **> Setup > Management**. Edit the Logging and Reporting Settings section and select the **Log Export and Reporting** tab and clear the check boxes for each report you want to disable.

New Management Feature	Description

CLI Find Command	The new `find command` CLI command helps you find a command when you don't know where to start looking in the hierarchy. This new command—which is available in all CLI modes—has two forms:
	• You can use `find command` alone to display the entire command hierarchy in the current command mode.
	Or
	• You can use `find command` with the `keyword` argument to locate all commands that have the specified keyword. For example, to find all configure mode commands with the `username` keyword, you would enter the following:
	`admin@mgmt-ui-4060#` **find command keyword username**
	`set deviceconfig system log-export-schedule <name> protocol ftp username <value>`
	`set deviceconfig system log-export-schedule <name> protocol scp username <value>`
	`set deviceconfig setting wildfire session-info-select exclude-username <yes|no>`
	`set mgt-config password-complexity block-username-inclusion <yes|no>`
	`set network interface ethernet <name> layer3 pppoe username <value>`
	`set shared certificate-profile <name> username-field`

Support for Syslog over TCP and SSL	The firewall and Panorama now support using TCP or SSL (default is UDP) for reliable and secure transport of logs to an external syslog server. SSLv3 and TLSv1 are supported and the default SSL port is 6514. To separate individual syslog messages in a TCP stream, the delimiter formats available are LF- Line Feed (BSD format, the default), and Message Length (IETF format). If the syslog server requires client authentication, you can configure the firewall/Panorama to use a certificate for secure communication. The option to mark a **Certificate for Secure Syslog** as available in **Device** (or **Panorama**) **> Certificate Management > Certificates > Device Certificates**. To monitor and alert you to a connection failure, a system log of high severity is generated when the firewall or Panorama is disconnected from the syslog server; an SNMP trap is also generated.
Support for Color-Coded Tags	Tags allow you to group objects using keywords/phrases and color (optional) to visually distinguish objects. You can apply tags to address objects, address groups (static and dynamic), zones, services, service groups, and policy rules. Use the **Objects > Tags** tab to create a tag, assign tag color, or to delete, rename and clone tags. When tagged, the keyword can be used to sort or filter objects.

New Management Feature	Description
SNMP Resource Monitoring Extensions	All Palo Alto Networks firewalls support SNMP objects that provide resource utilization and failure reporting, including alerts for hardware failure, the insertion and removal of the power supply, disks, or system fans, and monitoring of resource utilization for high session use or load on the gateway. The HOST-RESOURCES-MIB includes objects for monitoring the following: • Memory and disk usage on the management plane. Swap utilization tracks how the swap space is used to store all the running programs that aren't being actively used to free up memory. • Packet buffers on the dataplane. The Enterprise MIBs include objects for monitoring the following: • GlobalProtect gateway utilization in the PAN-Common MIB to monitor the total number of current active tunnels on the firewall device and the percentage on current tunnel utilization that is based on the number of active tunnels and the maximum number of tunnels allowed. • Session utilization in the PAN-Common MIB for each virtual system to track the active sessions, and the percentage of current session utilization based on session limit configured for the virtual system.
Enhancement in the Syslog Header	You can now choose the format of the hostname field in the syslog header. The syslog header can display one of the following: FQDN (hostname and domain name), hostname, the IPv4 address, or the IPv6 address of the sending device. Configure this option in the **Send Hostname in Syslog** drop-down on the **Device** (or **Panorama**) **> Setup > Management > Logging and Reporting Settings** section. The drop-down provides the following choices: **FQDN**, **Hostname**, **IPv4 address**, **IPv6 address**, or **None**; select **None** to leave the hostname field in the syslog header empty.

Networking Features

The following Networking features are introduced in PAN-OS 6.0. For more details about these features and for instructions on configuring them, refer to Networking Features in the New Features Guide.

New Networking Feature	Description
OSPFv3 Support	OSPFv3 provides support for the OSPF routing protocol within an IPv6 network. OSPFv3 offers similar structure and functionality to OSPFv2 (for IPv4). OSPPv3 and OSPFv2 can be run concurrently on the same firewall in a dual stack configuration. To configure a firewall to operate with OSPFv3, navigate to **Network > Virtual Routers** and then add or edit a virtual router configuration.
OSPF Graceful Restart	Reduces high availability (HA) active/passive failover times by allowing OSPF neighbors to continue using routes through a device during a short transition while out of service. This increases network stability by reducing the network outage experienced when OSPF adjacencies are reestablished. To configure a firewall to operate with OSPF Graceful Restart, navigate to **Network > Virtual Routers** and edit any OSPF or OSPFv3 virtual router configuration.

New Networking Feature	Description
IKE PKI Certificate Authentication for IPSec Site-to-Site VPNs	With this release authentication security has been enhanced over previous releases that only supported pre-shared-key authentication. To configure a firewall for IKE PKI certificate authentication, navigate to **Network > IKE Gateways** and then edit any IKE gateway configuration to select **Certificate** as the **Authentication** type and then specify which certificates to use for **Local Identification** and **Peer Identification**.
Decryption Port Mirror	Provides the ability to create a copy of decrypted traffic from a firewall and send it to a traffic collection tool that is capable of receiving raw packet captures—such as an RSA NetWitness or Solera Security Analytics Platform appliance—for archiving and analysis. This feature is necessary for organizations that require comprehensive data capture for forensic and historical purposes or data leak prevention (DLP) functionality. To enable use of this feature, you must download and install a free license. You can then configure a decryption profile (**Objects > Decryption Profile**) to enable forwarding to the decrypt mirror interface. Decryption port mirroring is available on the PA-7050, PA-5000 Series and PA-3000 Series platforms only.
TLS 1.2 Decryption	Previous releases of PAN-OS only supported TLS version 1.0. This release provides the Palo Alto Networks firewall with the ability to decrypt inbound sessions and forward proxy sessions that negotiate with TLS 1.2.
Increase Jumbo Frame Size	The maximum transmission unit (MTU) size has been increased to provide compatibility with equipment from other vendors. Jumbo frames must specifically be enabled at the global level. Once enabled, the default MTU size for all Layer 3 interfaces (the **Global MTU**) is set to a value of 9192 bytes, but can be configured for any value in the range of 512 - 9216 bytes. Because this value is applied globally, any other value required must be explicitly configured on a per-interface basis. To configure jumbo frame support, navigate to **Device > Setup > Session** and then select the **Enable Jumbo Frame** check box in the Session Settings dialog. After enabling jumbo frame support, you can customize the default MTU to be used globally and the minimum NAT64 MTU.
Remove TCP Timestamp	A new option has been added to the Zone Protection profile to enable you to strip the TCP timestamp from the TCP header.
IPv6 Neighbor Discovery Table Capacity Increase	In previous versions of the PAN-OS software, the Neighbor Discovery (ND) table was smaller than the ARP table for IPv4. With this release the IPv6 ND table size has been increased to account for larger IPv6 networks and implementation of v4/v6, dual-stack configurations.

New Networking Feature	Description
Enhanced Use for Address Objects	A Layer 3 interface on the firewall can now use an address object in lieu of an IP address. Using an address object allows you to separate the object from its value/IP address. The address object (**Objects > Addresses**) only has to be defined once and then it can be referenced multiple places in policy configuration. When the IP address(es) that was defined for the address object changes, you can edit the address object and the change in value is automatically inherited by all instances where the address object is used. For improved scalability, Panorama templates also allow you to add or select an address object when configuring a Layer 3 interface on the managed firewalls. Previously, when configuring a Layer 3 interface in a template you could not define a unique IP address for each managed firewall. With this new feature a template can reference an address object; the value for the address object can either be defined locally on the firewall or it can be defined as a shared object or as a device group object on Panorama. Defining the address object on the firewall allows you to configure a unique IP address for each managed device. To prevent a commit failure, you must create the address object on each firewall before pushing the template to the managed firewalls. Panorama templates support address objects in the following locations: • IP addresses for Layer 3 interfaces • Virtual address of the virtual IP address in a high availability (HA) active/active configuration • Service routes • NAT policy for source translation • GlobalProtect portal and gateway IP addresses • GlobalProtect satellite and site-to-site IP addresses • IKE Gateway local address • Multicast static and candidate IP addresses • BGP peer group local addresses • Hardware Security Module client IP addresses
Consolidation of Timers Used in a High Availability (HA) Setup	High availability (HA) timers are used to detect a firewall failure and trigger a failover. To reduce the complexity in configuring HA timers, three profiles have been added: **Recommended**, **Aggressive** and **Advanced**. These profiles auto-populate the optimum HA timer values for the specific firewall platform to enable a speedier HA deployment. Use the **Recommended** profile for typical failover timer settings and the **Aggressive** profile for faster failover timer settings. The **Advanced** profile allows you to customize the timer values to accommodate your network requirements. On upgrade, the current/existing HA settings are saved to the **Advanced** profile. If you prefer to load the preset values for the **Recommended** or **Aggressive** profiles, use the **HA Timer Settings** option in the **Election Settings** section of the **Device > High Availability** tab.

Panorama Features

The following Panorama™ features are introduced in PAN-OS 6.0. For more details about these features and for instructions on configuring them, refer to Panorama Features in the New Features Guide:

New Virtualization Feature	Description
Log Forwarding from Panorama	Panorama now allows for forwarding of aggregated logs, email notifications, and SNMP traps to external servers. Forwarding logs from Panorama reduces the load on the firewalls and provides a reliable and streamlined approach to combine and forward logs/SNMP traps/email notifications to external destinations. To facilitate this change the Panorama interface has been changed. See the Panorama Log Forwarding to an External Destination Per Platform table in the New Features Guide to configure log forwarding from Panorama:
Scheduling Dynamic Updates from Panorama	Dynamic updates for Application and Threats, WildFire, Antivirus, and URL Database can be scheduled using the **Schedules** link on the **Panorama > Device Deployment > Dynamic Updates** tab. The frequency of the updates, and the option to only download or to download and install updates to all managed devices and managed collectors using Panorama is configurable.
Support for PAN-DB and BrightCloud Databases	In deployments where both PAN-DB and BrightCloud databases are used concurrently for URL filtering, Panorama provides the capability to create shared policies and push the policies to devices running different databases. When a mismatch occurs between the URL database vendor configured on Panorama and what is configured on the device, the device now maps and auto-migrates URL categories and URL profiles so that the policies are relevant for the database enabled on the device.
Enhanced Use for Address Objects	See Enhanced Use for Address Objects feature in the Networking Features section.

User-ID Features

The following User-ID™ features are introduced in PAN-OS 6.0. For more details about these features and for instructions on configuring them, refer to User-ID Features in the New Features Guide:

New User Identification Feature	Description
Windows Server 2012/2012 R2 Support (Supported in PAN-OS 6.0.3 and later release versions)	You can now install the Windows-based User-ID agent on a system running the Windows Server 2012/2012 R2 operating system and you can now install the Terminal Server agent on a system running the Microsoft Windows Server 2012 R2 operating system. The User-ID agent that runs on the firewall can also integrate with Windows Server 2012/2012 R2 for user mapping and group mapping. The procedures to install the User-ID agent and Terminal Server agent and to configure user mapping are the same as for servers supported in earlier releases (Windows Server 2003 and 2008).

New User Identification Feature	Description
User-ID Integration with Syslog	In environments with existing network services that authenticate users, such as wireless controllers, 802.1x devices, Apple Open Directory servers, or other network access control (NAC) mechanisms, the firewall can now listen for syslog messages from those services so that the User-ID agent (either the Windows agent or the agentless user mapping feature on the firewall) can extract the authentication events from the log. Syslog filters that you define allow User-ID to parse the messages and extract the IP addresses and usernames of users who successfully authenticated to the external service and add the information to the IP address to username mappings it maintains. Previously you had to use the XML API in order to integrate with these external devices and extract this information.
Increased User-ID Active Users Limit	To support organizations with a large number of active users requiring IP address to username mapping for policy enforcement, the active user limit has been increased on the high-end firewall platforms based on the memory capacity of the individual platforms. The following list summarizes User-ID active limits on all Palo Alto Networks next-generation firewall platforms: PA-7050 and PA-5060: 256,000 PA-5050 and PA-5020: 28,000 PA-4000 Series, PA-3000 Series, PA-2000 Series, PA-500, and PA-200: 64,000
API Enhancement to Support Custom Terminal Service Solutions	The Terminal Services agent enables IP address to username mapping for users on Windows-based terminal servers by assigning a unique port range to individual users. The User-ID XML API has been extended to enable you to create scripts that allow for the same type of IP address to username mappings on non-Windows based terminal services. Specifically, the existing XML API calls that notify the firewall of IP address to username mappings have been extended to facilitate multi-user host log in and log off by including port mappings in addition to IP addresses.

Virtualization Features

The following virtualization features are introduced in PAN-OS 6.0. For more details about these features and for instructions on configuring them, refer to Virtualization Features in the New Features Guide:

New Virtualization Feature	Description
Virtual Machine (VM) Monitoring Agent	In previous releases, you had to use external scripts and the XML API on the firewall to furnish information about virtual machine IP addresses to the firewall. This feature allows you to dynamically retrieve changes in your virtualized environment without making configuration changes on the firewall. The Windows User-ID agent and the firewall can now be configured to proactively monitor the supported VM Sources: VMware ESXi server (4.1 and 5.0) and the VMware vCenter Server. The firewall supports up to 10 sources and the Windows User-ID agent supports up to 100 sources. In order to enable VM monitoring, the VM guest on the supported VM Sources must have VMware Tools installed and running. When you configure VM Information Sources on the **Device > VM Information Sources** tab, the firewall can access and retrieve the IP addresses of virtual machines (newly provisioned or modified) on the monitored sources. For each VM, you can also tag a predefined list of attributes. Each of these attributes can be used as match criterion in the new dynamic address groups feature and then referenced in policies. See Dynamic Address Groups for more details.

New Virtualization Feature	Description
Dynamic Address Groups	The Dynamic Address Groups feature allows you to dynamically update the network address of an object referenced in policy. Unlike a static address group where you specify the network address of a host, the members of a dynamic address group are populated using the match criteria that you define. The match criteria uses logical and or or operators; each host that you want to add to the dynamic address group must contain the tag that is defined in the match criteria. Tags can be defined directly on the firewall or on Panorama or they can be dynamically defined using the XML API and registered with the firewall. When an IP address and the corresponding tag (one or more) are registered, each dynamic group evaluates the tags and updates the list of members in its group. This capability allows you to add/ remove/update the members of a group without making any changes on the firewall; a commit is not required for policy to take effect when you provision new hosts or decommission existing hosts on your network. The dynamic address group will use the tags to populate its members. All matching tags-both static and dynamic-are evaluated to populate the group. The difference between static and dynamic tags is that statically added tags are part of the configuration on the firewall, and dynamically added tags are part of the runtime configuration. Because the members of the group are included based on the tags you match against, if an object has tags that match the specified criteria for the dynamic address group, the object will become a group member and the corresponding policy will be applied. For example, when provisioning a new server in a datacenter, you could tag the server's IP address as HTTP and DMZ. Using Dynamic Address Groups and the security rules on the firewall, the newly provisioned server would automatically be included in the existing policies to: • Allow incoming HTTP connections to all machines tagged as HTTP. • Allow all authenticated users to access all DMZ tagged machines through SSH and the web management console for the server. If you have a virtual environment with VMware, instead of using scripts to call the XML API, you can use the **Virtual Machine (VM) Monitoring Agent** to retrieve information (network address and corresponding tags) on new servers/guests deployed on the monitored hosts/servers. To learn about this feature, see Virtual Machine (VM) Monitoring Agent.
VM-Series on Citrix SDX	The VM-Series firewall is now supported on the Citrix SDX hardware platform running Citrix XenServer version 6.0.2 or later. Deploying the VM-Series firewall (one or more instances) on the SDX server provides the ability to consolidate the NetScaler VPX appliance and the Palo Alto Networks VM-Series firewall on the same physical platform and protect north-south and/or east-west traffic on your network. For a list of supported SDX platforms, deployment examples, and installation instructions, refer to Set Up a VM-Series Firewall on the Citrix SDX Server in the VM-Series Deployment Guide.

New Virtualization Feature	Description
Support for the VM-Series NSX Edition Firewall	Traditionally, the lack of context between the security and virtual environments made implementing security policies a challenge at the data center. To meet the security challenges in the software defined datacenter, Palo Alto Networks and VMware introduce a joint solution to safely enable all datacenter traffic, including intra-server virtual machine communications. NSX, the VMware Networking and Security platform that is designed for the software-defined datacenter, automates the process of deploying and provisioning the VM-Series firewall as a service (also called Security Virtual Machine) on ESXi servers. Refer to the table of components in the Support for the VM-Series NSX Edition Firewall section of the New Features Guide for information about the components of this joint Palo Alto Networks and VMware solution. To automate the process of deploying the VM-Series firewall, Panorama registers the VM-Series firewall as a service on the NSX Manager. The NSX Manager then deploys one VM-Series firewall on every ESXi host in a cluster. When a new ESXi host is added to the cluster, the NSX Manager automatically deploys a new firewall. Because each instance of the NSX edition of the VM-Series firewall is directly hooked in to the hypervisor, the firewall is seamlessly placed in the data path and can see all traffic that flows through the ESXi host. The NSX Manager and the VM-Series firewall work in concert to enforce security; each provides a set of traffic management rules that are applied to the traffic on each ESXi host. The first set of rules determines which traffic to direct to the VM-Series firewall on each host, and the second set of rules determines how the firewall must process-allow, deny, inspect, and constrain- the application for enabling it safely on your network. The tight integration of the NSX Manager, Panorama and the firewalls in this solution augments the ability to enforce consistent security policies using dynamic address groups. The NSX Manager updates Panorama of all changes in the virtual environment, and Panorama pushes the updates to the firewalls. All policy rules that reference these dynamic address groups are updated to reflect the changes in the virtualized environment and security policies are consistently applied to secure all network resources. To learn more about this solution refer to information about how to Set Up a VM-Series NSX Edition Firewall in the VM-Series Deployment Guide.

Changes to Default Behavior

The following is a list of changes to default behavior in PAN-OS 6.0:

- Added a new SSL root certificate in WF-500 6.0.12 for secure communication with PAN-OS and Panorama.

  December 1, 2015 is the expiration date for the previous certificate. You should update WF-500 appliances running release 6.0.11 or earlier releases to WF-500 6.0.12 or a later release to ensure successful communication with PAN-OS and Panorama after that date.

- After upgrading from a PAN-OS 5.0 release to a PAN-OS 6.0 release, interface errors are reported by SNMP monitoring tools. Although interface errors existed in PAN-OS 5.0 and earlier releases, firewalls running PAN-OS 5.0 releases did not display those interface errors using SNMP. Instead, SNMP monitoring tools displayed a value of `zero` for interface errors. A fix was added in PAN-OS 6.0 so that an SNMP monitoring tool displays interface errors with the correct values. Refer to the following KB article for more detail on this change: https://live.paloaltonetworks.com/docs/DOC-6864.
- If the Safe Search Enforcement option is enabled and the firewall has content update **422** or later installed, Safe Search enforcement will also apply to YouTube searches. With the Safe Search for YouTube, users will be able to search YouTube for videos, but if YouTube Safety Mode is not enabled, the user will not be able to watch any videos. The Safety Mode icon is located at the bottom of the YouTube.com page and will either show **Safety On** or **Safety Off**.
- The output for the `show session` command is modified to include tracker session information. A new line shows `tracker stage firewall` with the following possible values: `TCP RST-client`, `TCP RST-server`, `TCP FIN`, and `Aged out`.
- PAN-DB is now the default URL filtering database.
- The default value in the WildFire Server field (**Device > Setup > WildFire > General Settings**) is changed from `default-cloud` to `wildfire-public-cloud` in order to enable support for the WF-500 WildFire appliance.
- When creating a security policy, the policy will now by default match services running on the **application-default** port for the service rather than on an any port. The **application-default** setting prevents applications from running on unusual ports and protocols, which if not intentional, can be a sign of undesired application behavior and usage. Note that when you use this option, the firewall still checks for all applications on all ports, but with this configuration, applications are only allowed on their default ports/protocols.
- The GlobalProtect gateway client **Login Lifetime** is extended to enable configuration of the validity period an IKE security association (SA) for third-party IPSec clients connecting to GlobalProtect using the extended authentication (X-Auth) capabilities. Previously, the **Login Lifetime** field only controlled the length of time a GlobalProtect agent gateway login was valid. The SA for IPSec tunnels between a third-party VPN client and the gateway was valid for eight hours before requiring an IKE phase 1 re-key, and this SA lifetime was not configurable. Now, the GlobalProtect **Login Lifetime** set on the **Network > GlobalProtect > Gateways Client Configuration** tab controls both the amount of time a gateway login is valid (for GlobalProtect agents) as well as the amount of time the IPSec client SA with the gateway is valid. In addition, to enable support for IPSec clients that require a shorter key lifetime and to provide more configuration granularity for GlobalProtect agent configurations, the minimum value allowed for the **Login Lifetime** has been changed from 24 hours to two hours.
- If you enable the **Send Hostname in Syslog** (Logging and Reporting section of **Device > Setup > Management**) option, the default value used in the syslog header now is the fully qualified domain name (FQDN) which comprises the hostname and the domain of the device (firewall or Panorama) that sends the syslogs.

In PAN-OS 5.0, if the **Send Hostname in Syslog** was enabled, the syslog header contained the device's FQDN when both the hostname and domain were configured or just the hostname when the domain was not configured. If neither hostname nor domain was configured, the syslog header contained the IP address of the sending device.

In PAN-OS 4.1 and earlier versions, if the **Send Hostname in Syslog** option was enabled, the syslog header contained the IP address of the sending device.

Associated Software Versions

The following minimum software versions are supported with PAN-OS 6.0:

Palo Alto Networks Software	Minimum Supported Version with PAN-OS 6.0.0
Panorama	6.0.0
User-ID Agent	6.0.0
Terminal Services Agent	5.0.0
NetConnect	Not supported in 6.0
GlobalProtect Agent	1.2

Known Issues

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

Known Issues in PAN-OS 6.0

The following list describes known issues in the PAN-OS 6.0 release:

Starting with PAN-OS 6.0.15, 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.

Issue Identifier	Issue Description
—	While using Firefox version 30.0 with the Firebug add-on enabled, some aspects of the web interface and Panorama can be unresponsive. Workaround: Disable the Firebug plug-in or downgrade your Firefox version. You can also upgrade your Firefox browser—this incompatibility is a known issue in Firefox version 30.0 and is addressed in Firefox version 31.0.
84594	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 the firewall to use to perform DNS queries, services using the log card interface might not be able to generate DNS requests. This is only an issue if you've configured the firewall to use a service route for DNS requests, and in this case, you must perform the following workaround to enable communication between the firewall data plane and the log card interface. **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 `set deviceconfig system dns-setting dns-proxy-object`.
68588 This issue is now resolved. See PAN-OS 6.0.7 Addressed Issues.	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 `debug software restart management-server` CLI command.

Issue Identifier	Issue Description
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.
63854 This issue is now resolved. See PAN-OS 6.0.5 Addressed Issues.	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.
63186	If you perform a factory reset on a Panorama virtual appliance and configure the serial number, logging does not work until you reboot Panorama or execute the `debug software restart management-server` CLI command.
61720	By default, the GlobalProtect app adds a route on iOS mobile devices that causes traffic to the MDM server to bypass the VPN tunnel. **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**): • Add `0.0.0.0/0` as an access route. • Enter the IP address for the MDM server as an additional access route.
60851	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.
59749	On the Panorama web interface, the **Policies > Security > Post Rules > Combined Rules Preview** window does not display post rules and local rules for managed devices.
58202	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. **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.
58049	The Service dialog for adding or editing a service object in the web interface displays the incorrect port range for both source and destination ports: `1-65535`. The correct port range is `0-65535` and specifying port number 0 for either a source or destination port is successful.
57843	A file blocking profile configured with **continue-and-forward** as the action is not successfully sent to the WildFire cloud.
56434	When the GlobalProtect app accesses an MDM server through a Squid proxy, you must add the MDM server SSL access ports to the proxy server allow list. For example, if the SSL access port is 8443, add `acl SSL_ports port 8443` to the allow list.

Issue Identifier	Issue Description
49742	The following issues apply when configuring a firewall to use a hardware security module (HSM): • 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 a high availability (HA) configuration, the display of information from the `show ha-status` and `show hsm info` commands is blocked for 20 seconds.

Known Issues Specific to VM-Series Firewalls

- VM-Series on VMware vSphere Hypervisor (ESXi)
- VM-Series on Citrix SDX
- VM-Series on VMware NSX

VM-Series on VMware vSphere Hypervisor (ESXi)

Issue Identifier	Issue Description
62573 This issue is now resolved. See PAN-OS 6.0.3 Addressed Issues.	Upgrading a VM-Series firewall with the VM-1000-HV license can cause the firewall to go into maintenance mode without providing information about the cause. The VM-1000-HV license requires 5GB RAM on the VM-Series firewall due to the higher capacities supported by this license but this memory requirement is not enforced, which makes it possible to apply the VM-1000-HV license to a VM-Series firewall without enough memory allocated (default allocated memory is 4GB).
57321	After upgrading a VM-Series firewall to PAN-OS 6.0 on an ESXi host, issuing the `request shutdown system` command does not successfully shutdown the virtual firewall; the ESXi host continues to display the virtual firewall as powered on.

VM-Series on Citrix SDX

Issue Identifier	Issue Description
63282 This issue is now resolved. See PAN-OS 6.0.3 Addressed Issues.	A VM-Series firewall on a Citrix SDX server will not reboot into maintenance mode to allow administrators to perform specific tasks, such as reverting images or changing between FIPS and CC mode.
56452	On the Citrix SDX server, you must disable VLAN stripping on 1-gigabit ports assigned to the VM-Series firewall if you want to 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. With VLAN stripping disabled, the NetScaler VPX and the VM-Series firewall cannot share the same port. 10-gigabit ports work as expected and do not need to be altered.
52361	Adding or removing ports on the SDX server after deploying the VM-Series firewall can cause a configuration mismatch on the firewall. To avoid the need to reconfigure the interfaces, consider the total number of data ports that you require on the firewall and assign the relevant number of ports on the SDX server when deploying the VM-Series firewall. For example, if you assign ports 1/3 and 1/4 on the SDX server as data interfaces on the VM-Series firewall, the ports are mapped to eth1 and eth2. If you then add port 1/1 or 1/2 on the SDX server, eth1 will be mapped to 1/1 or 1/2, eth2 will be mapped to 1/3 and eth3 to1/4. If ports 1/3 and 1/4 were set up as a virtual wire, this remapping will require you to reconfigure the network interfaces on the firewall.

VM-Series on VMware NSX

Issue Identifier	Issue Description
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 Objects, from being available to Panorama. Workaround: To fix this issue, remove special characters from the password on the NSX Manager.
59856	After deploying the VM-Series firewall, when the firewall connects to Panorama, you must issue a Panorama commit to ensure that Panorama recognizes the device as a managed device. If you reboot Panorama without committing the changes, the firewall will not connect back to Panorama; although the Device Group will display the list of devices, the device will not display in **Panorama > Managed Devices**. Further, if Panorama is configured in a high availability (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: `vm-cfg: failed to process registration from svm device. vm-state: active`. This message is logged until you commit the changes on the active Panorama, which then initiates synchronization between the Panorama HA peers and the VM-Series firewall is added to the passive Panorama peer. Workaround: To reestablish the connection to the managed devices, commit your changes to Panorama (click **Commit** and select Commit Type: **Panorama**). In case of an HA set up, the commit will initiate the synchronization of the running configuration between the Panorama peers.
59573	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.
58839	When deleting the VM-Series deployment, all VMs are deleted successfully; however, sometimes a few instances still remain in the datastore. Workaround: Manually delete the VM-Series firewalls from the datastore.
58833	In some scenarios, traffic from newly added guests or virtual machines is not steered to the VM-Series firewall even when the guests belong to a Security Group and are attached to a Security Policy that redirects traffic to the VM-Series firewall. Workaround: Reapply the Security Policy on the NSX Manager.
58832	The VM-Series firewall fails to deploy with an error message: `Invalid OVF Format in Agent Configuration`. Workaround: Use the following command to restart the ESX Agent Manager process on the vCenter Server: `/etc/init.d/vmware-vpxd tomcat-restart`.
58260	If a high availability (HA) failover occurs on Panorama at the same time that the NSX Manager is deploying the NSX edition firewall, the licensing process fails with the error: `vm-cfg: failed to process registration from svm device. vm-state: active.` 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.
58170	When the datastore is migrated for a guest, all current sessions are no longer punted to the VM-Series firewall. However, all new sessions are secured properly.

Issue Identifier	Issue Description
58168	When deploying the VM-Series firewall, the Task Console displays: `Error while enabling agent. Cannot complete the operation. See the event log for details`. This error displays even on a successful deployment. You can ignore the message if the VM-Series firewall is successfully deployed.
57954	If you deploy the VM-Series firewall and then assign the firewall to a template, the change is not recorded in the bootstrap file. Workaround: Delete the Palo Alto Networks NGFW Service on the NSX Manager, and verify that the template is specified on **Panorama > VMware Service Manager**, register the service, and re-deploy the VM-Series firewall.
57614	When an ESXi host is rebooted or shutdown, the functional status of the guests is not updated. Because the IP address is not updated, the dynamic tags do not accurately reflect the functional state of the guests that are unavailable.
57533	The vCenter Server/vmtools displayed the IP Address for a guest incorrectly after vlan tags were added to an Ethernet port. The display did not accurately show the IP addresses associated with the tagged Ethernet port and the untagged Ethernet port. This issue was seen on some Linux OS versions such as Ubuntu.
57265	When editing a Security Policy with a network introspect rule, an `invalid (tcp) port number` error—or `invalid (udp) port number` error—displays when you remove the destination (TCP or UDP) port. Workaround: Delete the network introspect rule and create a new one.
57205	When defining traffic introspection rules (to steer traffic to the VM-Series firewall) on the NSX Manager, either the source or the destination for the rule must reference the name of a Security Group; you cannot create a rule from any to any Security Group. Workaround: To redirect all traffic to the VM-Series firewall, you must create a Security group that includes all the guests in the cluster. Then you can define a security policy that redirects traffic from the cluster and to the cluster.
57203	Duplicate packets are being punted to the VM-Series firewall. This issue occurs if the distributed vSwitch used for punting is enabled in promiscuous mode. Workaround: Disable promiscuous mode.
55586	When adding or removing a Security Group (Container) that is bound to a Security Policy, Panorama does not get a dynamic update of the added or removed Security Group. Workaround: On **Panorama > VMware Service Manager**, click the **Synchronize Dynamic Objects** link to initiate a manual synchronization to get the latest update.
55393	Dynamic Tags (update) do not reflect the actual IP address set on the guest. This issue occurs because the vCenter Server cannot accurately view the IP address of the guest.

PAN-OS 6.0.15 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.15 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

Starting with PAN-OS 6.0.15, 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.

If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	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-57659	A security-related fix was made to address a cross-site scripting (XSS) condition in the web interface (PAN-SA-2016-0031).
PAN-56221	A security-related fix was made to address a cross-site scripting (XSS) condition in the web interface (PAN-SA-2016-0033).
PAN-55477	A security-relarted fix was made to address CVE-2016-0800 (DROWN), CVE-2016-0703, and CVE-2016-0704 (PAN-SA-2016-0030).
PAN-55259	A security-related fix was made to address multiple NTP vulnerabilities (PAN-SA-2016-0019).
PAN-55237	A security-related fix was made to address an XPath injection vulnerability in the web interface (PAN-SA-2016-0037).
PAN-55122	A security-related fix was made to address CVE-2015-7547 (PAN-SA-2016-0021).
PAN-52379	A security-related fix was made to address CVE-2015-5364 and 2015-5366 (PAN-SA-2016-0025).
PAN-52038	A security-related fix was made to address a cross-site scripting (XSS) condition in the web interface (PAN-SA-2016-0029).

PAN-OS 6.0.14 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.14 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

> ⚠ If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
95622	Security-related fixes were made to address issues identified in the May 3, 2016 OpenSSL security advisory (PAN-SA-2016-0020).
93612	A security-related fix was made to address a privilege escalation issue (PAN-SA-2016-0015).
93072	A security-related change was made to address an issue in the policy configuration dialog (PAN-SA-2016-0014).
92413	A security-related change was made to address a boundary check that caused a service disruption of the captive portal (PAN-SA-2016-0013).
92293	A security-related fix was made to address CVE-2016-1712 (PAN-SA-2016-0012).
89984	A security-related fix was made to address a stack overflow condition (PAN-SA-2016-0024 -89984-WebUI-DoS).
88191	A security-related fix was made to address information leakage in systems log that impacted the web interface (PAN-SA-2016-0016).
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).

PAN-OS 6.0.13 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.13 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
89962	An update was made to ensure that firewalls and appliances running PAN-OS 6.0.13 and later PAN-OS 6.0 releases meet the transition requirements for random number generators (RNGs)—such as the X9.31 RNG—provided in SP 800-131A. The X9.31 RNG is replaced by the CTR_DRBG specified in SP 800-90A.
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.
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.
77163	Fixed an issue where the `/var/log/secure` 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.
67207	Fixed an issue where an upgrade to a PAN-OS 6.0 release caused the dataplane to stop responding.

PAN-OS 6.0.12 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.12 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

⚠ If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
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 6.0 release to PAN-OS (or Panorama) 6.0.12 or a later release.
85721	Fixed an issue where firewalls with a specific OCZ Deneva hard disk (model DENCSTE251M21) configured in a RAID and running PAN-OS 6.0.9 or later releases experienced RAID errors.
85065	Fixed a CLI input parsing issue that caused a process on the management plane to stop responding when processing unexpected input.
83519	A security-related fix was made to address CVE-2015-5600.
81367	A security-related fix was made to address CVE-2015-4024.

PAN-OS 6.0.11 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.11 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
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 `User admin logged in via Panorama from x.x.x.x using http` regardless whether the connection was encrypted. With this fix, the System log now specifically reports `User admin logged in via Panorama from x.x.x.x using http over an SSL connection` when the administrator is connected through an encrypted SSL connection to differentiate from non-encrypted connections.
79443	Fixed an issue in the web interface where, in some cases, the PHP session cookie (PHPSESSID) was not marked as secure.
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.
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 *trie* (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.
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 `show session meter` CLI command.
78304	A security-related fix was made to address a cross-site request forgery (CSRF) issue in the web interface.
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 `Required client certificate is not found` even when the certificate was available.

Issue Identifier	Description
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**.
76711	Fixed an issue where the dataplane stopped responding on a device using a shared gateway with Captive Portal in redirect mode.
76615	Fixed an issue on a PA-7050 firewall where running the `request system private-data-reset` command when there was a faulty disk drive on the Log Processing Card (LPC) caused an LPC failure during reboot.
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.
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.
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 `return-mac ager` lists, which caused the restarts. With this fix, the firewall retrieves and checks return MAC entries to avoid this race condition and associated restarts.
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.
73878	Fixed an intermittent issue where BGP failed to redistribute the static Discard routes as expected after a high availability (HA) failover.
71674	Fixed an issue for firewalls running PAN-OS 6.0 releases where the SSL VPN process (*sslvpn*) restarted with a core dump due to a null pointer.
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 `debug management-server report-namelookup` command to work around this issue by disabling DNS name lookups in reports.
70919	Fixed an issue where the dataplane in a high availability (HA) active/active configuration restarted when a `session update/remove` 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 `session update/remove` message while waiting for those results.
66681	Resolved a dataplane restart issue due to race conditions.
65370	Fixed an issue where log queries utilizing DESC order or neq operator would not return expected results on M-100 or PA-7050

Issue Identifier	Description
64266	Fixed a rare issue where certain processes (*l3svc* and *sslvpn*) stopped responding when a Content update and FQDN refresh occurred simultaneously.
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`.
59914	Fixed an issue where the firewall did not remove the pan_task_x.log or .log.old files as expected when executing the `debug dataplane packet-diag clear log log` command.

PAN-OS 6.0.10 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.10 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

> ⚠ If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
78897	Fixed an issue where excessive ZIP traffic caused a null pointer exception in ZIP processing software, causing the dataplane to stop responding.
78206	Fixed an issue where a multi-dataplane platform did not properly free SSL 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 in PAN-OS 6.0.9 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**.
77237	Fixed an issue where some PA-200 firewalls failed to boot when rebooted or power-cycled after a single PAN-OS software upgrade. You can work around this issue by performing two complete software upgrades, which corrects both u-boot images in the boot flash. With this fix, PA-200 firewalls can be upgraded to PAN-OS release 6.0.10 or higher releases and then rebooted or power-cycled normally without the need to first perform two consecutive upgrades.
76238	A security-related fix was made to address CVE-2015-1873.
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.
75905	Fixed an issue where a firewall failed to download the BrightCloud database via proxy after upgrading to either PAN-OS 6.0.8 or PAN-OS 6.0.9.
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.
74735	Fixed an issue where a PA-7050 dataplane restarted when attempting to process jumbo frame packets (larger than 1,500 bytes).
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.

Issue Identifier	Description
74138	Fixed an issue where some PA-7050 firewalls in high availability (HA) mode experienced packet buffer leaks in PAN-OS 6.0 or higher releases. The leaks occurred when interface tables, configurations, or IDs on the two HA devices lost synchronization and HA session sync messages included interface attributes that did not exist on the receiving device. Leaks also occurred when the HA pair was upgraded from PAN-OS 6.0 to PAN-OS 6.1 and interface IDs were out of sync during the time the two firewalls were not running the same software version. With this fix, packet buffer leaks caused by unsynchronized interface attributes 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.
73689	Fixed an issue where traffic interruptions occurred due to nested encoding (ZIP content within chunked encoding), which caused the `SML VM vChecks` buffer pool to overflow. With this fix, new checks have been added to prevent `SML VM vChecks` 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 `idmgr reset` command for type `user`.
73180	Fixed an issue where, with Strip X-Forwarded-For (XFF) enabled under **Device > Setup > Content-ID**, an XFF 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.
72737	Fixed a memory corruption issue that caused the dataplane to restart when SSL decryption was enabled.
70669	Fixed an issue where the User-ID process crashed due to bulk and incremental updates of terminal server users on the active-secondary device in a high availability (HA) active/active configuration.
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.
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.
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.
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.

Issue Identifier	Description
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.

PAN-OS 6.0.9 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.9 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

⚠ If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
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.
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.
73813	When using the PAN-OS® CLI in configuration mode, the `show predefined signature` CLI command incorrectly displayed App-ID™ signatures and patterns for some predefined applications. The `signature` command option has been removed and the `show predefined` command now correctly displays application information, but does not display the App-ID signature and pattern.
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.
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.
73071	Fixed an issue where the firewall incorrectly sent duplicate SYN packets for ftp-data sessions.
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 to avoid traffic interruptions.
72763	Fixed an issue where HA3 packet forwarding may fail in a high availability (HA) active/active configuration when using an Aggregate Ethernet (AE) subinterface to send and receive traffic.

Issue Identifier	Description
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.
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.
72536	Fixed an issue where packet buffers leaked when a firewall with inbound SSL decryption 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.
72285	New counters have been added to track the upload process for files forwarded to WildFire.
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.
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 link down state.
70903	Fixed an issue where SNMP traps from some firewalls were not parsed correctly by the SNMP manager.
70816	Fixed an issue where the `Address is not valid` error displayed when running commands that initiate a filtering session based on an IPv6 address (examples of the affected commands include `clear session all`, `set application dump`, and `test decryption-policy-match`). IPv6 address validation now works correctly.
70544	A dataplane restart occurred when the **SSL 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 SSL decryption is enabled.
70304	Resolved an issue that was seen with **Rematch Sessions** enabled, where a race condition could occur when new security policies were matched to existing sessions.
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.
69900	Fixed an issue where the tech support file did not contain some expected files, including /var/log files.
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 was full. This issue has been fixed so that stale IPv6 neighbor entries are correctly removed when the neighbor table threshold is reached.

Issue Identifier	Description
69242	When a user failed to authenticate using the web interface, firewall system logs did not display the user'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 `general` event and displays only the username of the user who failed authentication. The other entry is logged as an `auth-fail` event and displays both the username and source IP address of the user who failed authentication.
68982	Fixed an issue where the firewall stops receiving new reports from WildFire when the report ID on the WildFire public cloud exceeds a certain limit. (WildFire continues to generate reports but does not log them as expected on the firewall).
67930	Fixed an issue where an update to a stale IPv6 neighbor entry could cause a dataplane restart.
67810	When a PA-5000 Series device initiates sessions on different data planes in an environment with multiple virtual systems, session traffic sometimes 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.
66217	Fixed an issue that caused unreliable VoIP communication. The issue occurred for firewalls in a high availability (HA) active/active configuration, and was due to predict session traffic not being installed correctly on the HA peer when the peer was setup to use a dataplane other than DP0 to process the session.
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 avail-able for ping requests and keep-alive messages even when under an unusually heavy load.
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 using the same interface on which it arrived, was dropped with the message `Symmetric Return: Packet dropped, no return MAC found.` The issue is fixed.

PAN-OS 6.0.8 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.8 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

> If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
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.
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 work correctly. This issue has been fixed so that HA peers will sync correctly following an upgrade.
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 by the firewall. This issue has been fixed so that following a firewall restart, any OSPF adjacency remains established.
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.
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 address 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.
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.
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.

Issue Identifier	Description
71486	A fix was made to address an issue with user input sanitization to prevent Cross-site Scripting (XSS) attacks against the web interface.
71464	If the firewall initiates a point-to-point protocol over Ethernet (PPPoE) session, an issue was seen when a server responds with a PPPoE 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.
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 addressed objects, and address object names are displayed consistently.
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.
70499	Fixed an issue where traffic that 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.
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.
69934	Fixed an issue where active File Transfer Protocol (FTP) enabled with Dynamic IP Network Address Translation (NAT) failed. Inconsistent translation was seen for PORT packets sent over the control connection established between the FTP server and the NAT device.

Issue Identifier	Description
69685	Updates were made to existing Russian time zones and new Russian time zones were added to the available list of global time zones for a device, to accommodate the 2014 changes to Russian time zones.
69528	An issue was seen with captive portal enabled in an environment with multiple virtual systems, where two virtual systems were configured as User-ID collectors. When captive portal timed out a User-ID entry in one virtual system, captive portal did not time out for the same User-Id entry in the second virtual system, and the user was not prompted to re-authenticate to the captive portal login page. This issue has been fixed so that if captive portal times out for a User-ID entry in one virtual system, the same User-ID entry correctly times out in the second virtual system and the user is prompted to authenticate to the captive portal login page.
68764	When a DNS 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.
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 Duplicate group name and this issue has been resolved so that pushing a user group from Panorama to a managed firewall works correctly.
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 (**Objects > Custom Objects > Vulnerability**). 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.
68372	Setting up a static MAC configuration for a tagged interface configured on a VLAN did not work correctly. This occurred when 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.
68100	The Strip X-Forward-For (XFF) feature did not correctly remove the contents of the XFF header field when the HTTP GET request contained encoded URL characters. This issue has been fixed to ensure that the Strip XFF feature removes the contents of the XFF field from the HTTP header, including when the HTTP GET request contains encoded URLs.
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 a PAN-OS 6.0 release version, in some cases 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 version and restarting the firewall.

Issue Identifier	Description
67567	When a new version of the BrightCloud URL database was downloaded and installed, if the category for a URL changed in the new version of the database from the previous version, the change in category was not reflected on the dataplane. With this fix, URL categories on the dataplane are updated correctly after a installing a new version of the BrightCloud database.
65477	A deadlock issue has been addressed where an inter-process communication (IPC) failed while another IPC operation was in progress. This resulted in the management server restarting with a core dump.
64958	Resolved an issue displayed on the Panorama web interface, where the **Oldest Log** statistics incorrectly showed no data (**Panorama > Managed Collectors > Collector Statistics**).
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.
64600	When a dynamic block list was configured on the firewall to be updated according to a list hosted on a web server, the firewall was configured to access the web server using a proxy server. An issue was seen where the firewall was connecting directly to the web server hosting the block list, instead of using the proxy server to connect to the web server. This issue has been fixed so that when a proxy server is configured, the firewall updates the dynamic block list using the proxy server and does not connect to the server hosting the block list directly.
64040	The logging partition could become full on a log collector if the total configured quota was larger than 90%. A fix was made to address the way free space is allocated for the logging partition.
62791	An update was made to reduce the number of TCP stale sessions for PA-5000 Series devices.
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.
58055	Addressed an issue where a race condition between a high availability (HA) synchronization and a web interface commit caused a management server restart.
55249	You can now run the `test <feature>` CLI command 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 6.0.7 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.7 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

> ⚠ If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
70588	Fixed an issue where a browser with Transport Layer Security (TLS) 1.2 enforced could not access the GlobalProtect™ portal login page. This issue occurred when no client certificate was configured.
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.
69956	Resolved an issue where NetFlow information for some sessions was not being forwarded for PA-5000 Series devices due to a session ID format change.
69035	When using the **ACC** tab on the Panorama™ web interface to view statistics for a custom application, using applications filters (such as Category, Subcategory, and Technology) to filter the data displayed for the custom application 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.
68836	In a a high availability (HA) configuration, a path monitoring failure lead to a delayed HA failover. An update has been made to optimize HA failover time.
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 on a managed firewall are still displayed correctly after establishing a connection with Panorama.
68472	Addressed an issue where some expected counters were not returned in the output for the `<show> <interface>` XML API command for loopback, VLAN, and tunnel interfaces.
68389	The Application subcategory 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.
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.

Issue Identifier	Description
67856	When a primary NTP server was down and the secondary NTP server was up, the CLI incorrectly showed the secondary NTP server as down. This has been fixed so that the CLI displays the correct status for both the primary and secondary NTP servers.
67833	When a tech support file was generated for 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 a space in the device group name 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 that 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.
67778	Fixed an issue where a GlobalProtect Mac client experienced intermittent connectivity with the GlobalProtect portal when running Mac OS X 10.10.
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.
67300	Addressed an issue on the VM-Series firewalls where enabling packet capture for certain application-level gateway (ALG) traffic causes the system to restart.
67268	A DNS sinkhole was not responding to DNS queries that contained DNSSEC Header flags, such as the Authenticated Data (AD) bit or Checking Disabled (CD) bit. The DNS sinkhole now correctly responds to DNS queries that contain DNSSEC header flags (AD or CD bit) and the firewall can successfully provide the DNS sinkhole IP address to the client.
67258	The process (*mprelay*) 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 mprelay process to restart. With this fix, the IPv6 ND performs correctly and avoids unexpected restarts of the mprelay 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: `Abnormal system memory usage detected, restarting userid with virtual memory`. 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.
67160	An issue was fixed where a data port configured on a PA-7050 firewall as a Log Card Interface was restarting when commits were performed.
66924	When logging in to the Panorama web interface with two-factor RADIUS authentication, Panorama would successfully authenticate an administrator but then immediately log the administrator out of the web interface. With this fix, Panorama no longer logs the administrator out of the web interface following a successful authentication.

Issue Identifier	Description
66918	Memory corruption issues related to SSL decryption caused the dataplane to restart and resulted in a flapping condition between firewalls in an HA cluster.
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, causing an error on the client.
66482	In some cases, the web interface was not accessible for an M-100 appliance even though the appliance could be accessed through the CLI. This issue is the result of a race condition, where a reporting process attempted to delete session that had been previously deleted. This issue is not addressed so that the web interface and CLI are both accessible for an M-100 appliance.
66364	Fixed an issue that prevented two certificates with the same subject name from being installed following an upgrade to a PAN-OS 6.0 release version.
66208	A brute-force attack on an unprotected management interface on the firewall caused the /var/log/btmp 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.
66161	For a PA-3050 firewall, the next hop MAC address for hardware offload did not update correctly for routes that were learned using multiple dynamic routing protocols. This occurred when the routing protocols were not using the default administrative distance. Packets used the wrong egress interface when the session was offloaded. This issue has been resolved.
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.
65180	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.
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 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 fallback to a lower TLS version. With this fix, fallback to a lower TLS version succeeds with Google Chrome and Mozilla Firefox. A specific behavior of Internet Explorer still exhibits issues.
64223	Fixed an issue where FQDN objects that were added to a dynamic address group were not listed after issuing the `request system fqdn show` command, with the command displaying a message that no FQDN object is used in the policies.
63150	In an Active/Active HA setup, 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.
61056	IPSec tunnels could not be established due to the firewall running out of encap/decap context. An enhancement was made to allow more granular debugging for the depletion of encap/decap context for IPSec tunnels, in order to provide further root cause analysis. Restart the firewall as a workaround for this issue.

Issue Identifier	Description
60617	TCP connectivity issues occurred on a virtual machine when SYN Flood was enabled with the SYN Cookies **Activate Rate** set to zero. This was due to an issue where active and passive FTP were not working under different NAT configurations, and has been addressed so that both active and passive FTP work correctly under different NAT configurations and do not cause TCP connectivity issues. A workaround for this issue is to set the **Activate Rate** to a value greater than zero (**Objects > Security Profiles > DoS Protection > Flood Protection > SYN Flood**).

PAN-OS 6.0.6 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.6 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

⚠ If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
68899	Fixed an issue that affected PA-7050 firewalls. An HSCI port configured as an HA2 interface went down due to a dataplane board restarting. An improvement has been made so that if more than one dataplane board is installed, an HA2 interface on an HSCI port will stay up.
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.
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 process that was restarting when the password was configured. This issue has been fixed.
67910	While viewing the **Combined Rules Preview** on the Panorama™ web interface (**Policies > Preview Rules > Combined Rules Preview**), the **Device** drop-down displayed the virtual system number for some virtual systems and not the virtual system name. This issue has been fixed so that the **Device** drop-down in the Combined Rules Preview displayed the names of the virtual systems that you can select.
67873	Resolved an issue where disabling OSPF and performing a commit caused a routing process to restart. This was due to a race condition related to running the `show route` command during a commit.
67860	On the Panorama web interface, the **Preview Changes** button could not be clicked when **Group HA Peers** was selected. This has been fixed so that the **Preview Changes** button is correctly enabled when **Group HA Peers** is selected (**Panorama > Templates**).
67723	Fixed an issue that occurred when an OSPF profile was configured with a tunnel interface and the **Passive** state was disabled for the tunnel interface. In this case, the runtime configuration incorrectly overrode the configured settings, and the tunnel interface was incorrectly enabled as **Passive**.
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.
67483	This fixes an issue where a firewall failed to email scheduled reports due to a race condition.
67436	The `debug software trace reportd` and `debug software core reportd` commands were added to the CLI command structure.

Issue Identifier	Description
67399	Fixed an issue that occurred in a high availability (HA) active/active configuration, where log card interfaces were synced to the HA peer and resulted in duplicate IP addresses.
67344	Fixed an issue for the M-100 appliance where the `show log-collector detail` command was presenting incorrect information.
67069	Internal packet path monitoring failure errors caused the dataplane to restart. An enhancement was made to detection and recovery mechanisms to minimize the impacts of these errors.
66959	Addressed an issue where configuring overlapping IPv6 addresses when adding a **OSPFv3 range** on the **Network > Virtual Routers > OSPFv3 > Area > Ranges** tab caused a restart to occur after attempting to commit. This issue has been fixed so that if an invalid range is entered, an error is displayed; if a valid range is entered, you can continue to commit successfully.
66690	The dataplane restarted due to a process restart while running traffic in a high availability (HA) configuration. Additional checks have been added to avoid a possible race condition, which had led to the dataplane process restart.
66503	Addressed an issue where the firewall dataplane experienced an out of memory condition, which could cause the dataplane to restart and the firewall to go into nonfunctional state.
66466	Addressed an issue for PA-2000 Series firewalls, where a device failed to handle a 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.
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).
66168	Resolved an issue where adding an FQDN to the Servers table to specify an LDAP server in an LDAP server profile caused intermittent connection issues (**Device > Server Profiles > LDAP**).
66025	Configuration files with names longer than 32 characters were allowed and could be successfully imported, but load and delete operations would fail. With this fix, configuration file names of up to 32 characters can be imported and configuration files with longer names are prevented from being imported with an error.
65607	If the last remaining user was removed from the **Allow List** for an LDAP authentication profile (meaning no users remained on the list), authd was not notified that the group was empty and retained the last user's information. That user could continue to be authenticated despite no longer being included in the allow list. This has been addressed so when the last user remaining on the allow list is removed, the user can no longer authenticate.
65565	Fixed an issue where selecting R**eplay attack detection** in the **GlobalProtect gateway satellite** configuration on the web interface did not actually enable replay attack detection.
65488	Resolved an issue that occurred with a high availability (HA) active/passive configuration, where using the `request -availability state suspend` command to suspend the active peer and perform an HA failover resulted in some packet loss.

Issue Identifier	Description
65176	Resolved an issue that caused a dataplane restart on the VM-Series firewall, when using RC4 ciphers to decrypt SSL traffic. This issue is specific to ESXi servers using AMD processors.
64647	Following an upgrade from a PAN-OS 5.0 release version to a PAN-OS 6.0 release version, high availability (HA) synchronizations were failing intermittently. The HA sync failures were due to an issue where the host information profile (HIP) database was not syncing correctly during the HA sync between the peers. This issue has been fixed so that performing a HA synchronization works correctly.
64379	This fixes an issue where older cached IP address to username mappings on a User-ID agent could overwrite newer IP address to username mappings on the firewall. With this fix, IP address to username mappings with more recent timestamps take precedence over IP address to username mappings with older timestamps.
64309	A WildFire™ threat log with the severity `Informational` was incorrectly showing the severity `Emergency` when forwarded to a syslog server. This issue has been fixed so that when WildFire logs are forwarded to a syslog server, the log entries show the correct severity for the log.
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.
58820	On PA-5000 Series firewalls, Static Source NAT, Dynamic IP NAT, and Destination NAT session processing has been enhanced to greatly improve the throughput in these NAT scenarios, allowing the firewall to use multiple CPUs to process NAT sessions, rather than anchoring the sessions to a CPU based on destination IP hash.

PAN-OS 6.0.5-h3 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.5-h3 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

⚠ If you have asymmetric routes in your network or have attached a zone protection profile, before you upgrade to PAN-OS 6.0.5-h3 or a later PAN-OS 6.0 release, you must review the important notes in the Upgrade to PAN-OS 6.0 section of the PAN-OS 6.0 New Features Guide.

Issue Identifier	Description
69173	Under certain conditions, unspecified layering of packet-level evasions could be used to bypass signature matching of the session.

PAN-OS 6.0.5 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS 6.0.5 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

Issue Identifier	Description
68018	When configured in high availability (HA) mode, the High Speed Chassis Interconnect (HSCI) ports using QSFP modules on the PA-7050 experienced packet loss. This HSCI link flapping issue has been resolved.
67613	Resolved an issue where uploading files to Wildfire sometimes failed when the files were uploaded from the client to the server using HTTP.
67565	For Panorama and PAN-OS, when an Admin Role Profile was set up with Privacy permissions disabled, the administrator was able to search the traffic logs based on username. This issue has been fixed so that an administrator without privacy permissions cannot search traffic logs based on username.
67378	Resolved an issue where LEDs for copper ports on the PA-7050 firewall that were configured as high availability (HA) ports were not correctly showing active links.
67246	Resolved an issue where modifying an existing policy caused any tags configured in that policy to be removed.
67073	Fixed an issue where link flapping was seen during a high availability (HA) failover.
67058	Resolved an issue where a Vulnerability Protection profile did not match a custom vulnerability signature when the vulnerability name was entered as the **Threat Name** in the vulnerability protection rule. This issue has been resolved so that the Vulnerability Protection profile matches signature when the vulnerability name is entered as the Threat Name in the rule. As a workaround, the **Threat Name** in the Vulnerability Protection profile could be set to **any** so that the profile will match the custom signature.
66910	With Block Password Change Period enabled to specify an amount of time during which an administrator cannot change a password, an administrator's password could still not be changed after the period had passed. This has been resolved so that when the period has passed, a password for an administrator can be successfully modified.
66692	Resolved an issue where device administrators with privacy settings disabled were still able to view usernames on the **ACC** tab.
66610	Scheduled email reports for Panorama were not correctly showing IP addresses resolved to hostnames, and were continuing to display IP addresses for entries. This issue has been resolved so that hostnames are correctly displayed in scheduled email reports instead of the corresponding IP address.
66342	Resolved an issue that occurred with Panorama peers in a high availability (HA) configuration. Following an HA failover, a managed device forwarded logs to the secondary Panorama while the primary Panorama was down. When the primary Panorama came back online, the managed device incorrectly continued to forward logs to the secondary Panorama. This has been fixed to ensure that managed devices correctly forward logs to the primary Panorama when both the primary and secondary Panoramas are online.

Issue Identifier	Description
66215	Resolved an issue that caused a dataplane restart when a tech support file was being generated and a content update was being performed at the same time.
66199	When the option **Target to all but these selected devices** was enabled for a Panorama Security policy, the policy was being pushed to the dataplane of managed devices that were explicitly excluded from receiving the policy (the policy should not have been pushed to these devices at all). This issue has been fixed so that when **Target to all but these selected devices** is enabled, the policy is correctly pushed to devices associated with that policy, and is not pushed at all to devices that are explicitly excluded.
66043	A PA-5050 firewall was showing that it only supported 32,768 device routes when it should support a maximum of 64,000 routes. This issue has been resolved to ensure that the firewall supports 64,000 device routes.
65936	Addressed an issue where the device server could crash if a configuration referenced different names for a single GlobalProtect gateway entry.
65905	Addressed an issue where a routing process restarted, causing the firewall to restart. This occurred when configuring virtual routers with both OSPF and BGP enabled with aggregate routes and routes to be redistributed.
65833	In a high availability (HA) active/active configuration, resolved an issue where the primary HA device did not resume the primary status after being suspended, when the preemptive option was enabled on both firewall peers in the setup.
65828	On Panorama, with the option to **Share Unused Address and Service Objects with Devices** enabled, certain conditions caused unused objects to still be pushed to managed devices. This issue has been fixed so that unused objects are not pushed to firewalls when the option to **Share Unused Address and Service Objects with Devices** is not selected.
65801	Traffic for a voice and video application was being dropped because Network Address Translation (NAT) was not correctly translating the application's IP address and the traffic was not able to be routed correctly. This issue has been resolved so that H225 and H245 traffic is handled efficiently by the firewall-NAT is correctly performed for voice and video applications and calls placed using Voice over IP (VoIP) do not fail.
65765	Addressed an issue related to parsing long URLs which in some cases was causing an infinite loop that could cause the dataplane to restart.
65747	When one port configured as a virtual wire interface was brought down and then brought back up, both virtual wire interfaces continued to flap before stabilizing. This was an issue for 10G Fiber ports and has been resolved.
65678	After upgrading to Panorama 6.0.0 or a later release version, previously authenticated non-local administrator accounts, like RADIUS authenticated administrators, could not log in using the CLI unless first logging in to the web interface. This issue has been addressed so that, following a Panorama upgrade, an authenticated administrator can successfully log in to the CLI without first logging in to the web interface.
65511	The Mozilla compatibility user agent headers in Internet Explorer 11 were changed, causing Captive Portal to identify Mozilla as an unsupported browser and NTLM authentication was not performed. This issue has been resolved so that Internet Explorer 11 can perform NTLM authentication.

Issue Identifier	Description
65496	The Panorama command line interface (CLI) was displaying an extra line when exiting the CLI when running Panorama 6.0.2 or 6.0.3. The additional line, which indicated that the management session was terminated, was not displayed in releases prior to Panorama 6.0.2 and has been removed.
65340	A commit failed without a clear error message when a static route statement overlapped an OSPF export statement. Updates have been made to clarify the error message showing conflicts that could lead to a failed commit.
65292	Safe Search Enforcement was not being enforced when users were logged into either Bing or Google accounts (if users were logged out of their Bing or Google accounts, Safe Search enforcement worked correctly). This issue has been resolved so that Safe Search Enforcement blocks Bing or Google search results correctly, even when users are logged into Google or Bing accounts.
65256	The system logs on a PA-7050 displayed an error informing the user that an executable file could not be found. This issue has been fixed so that the executable file has a valid file path and the error is no longer displayed.
65068	Resolved an issue seen while forwarding logs to a syslog server, where the `risk-of-app` field was displayed as an application instead of a risk value.
64990	Attempting to sort entries for scheduled custom reports according to the **Receive Time** under **Monitor > Reports** was not the correct sorted results. This has been fixed so that these results can be correctly displayed in ascending or descending order by **Receive Time**.
64908	With both OSPF and BGP enabled, if OSPF was configured to redistribute the default route `0.0.0.0/0`, this caused OSPF to redistribute routes that were configured for BGP route redistribution. Resolved this issue so that OSPF no longer redistributes routes configured for BGP redistribution.
64707	Fixed an issue where a device server process restarted unexpectedly while processing the URL cache.
64705	Exporting logs from Panorama and then attempting to import them to a managed device did not display the logs on the managed device. Imported logs were placed in a temporary directory before being added to the main database. An ordering error in this process was cleaning up the temporary directory before the imported logs were correctly merged into the main database. This issue has been resolved.
64664	Resolved an issue where the Detailed Log View for traffic logs was not displaying the Log Links widget (**Monitor > Logs > Traffic**).
64642	Fixed an issue where an IP address obtained from a DHCP server on a dataplane interface was not binding to the dataplane and an IP address obtained from a PPPoE server on a dataplane interface was not bound to the dataplane. This issue has been resolved.
64596	A user icon was showing for a group object, when the group object was added to a security policy. This has been fixed so that a group icon is shown for a group object when added to a security policy.
64550	Resolved an issue where enabling NAT64 resulted in unexpected ARP behavior on Layer 3 interfaces.
64165	Following a Panorama upgrade to PAN-OS 6.0.2, several duplicated email notifications were being sent for old logs. This was due to an issue with sequence and acknowledgment (SEQ/ACK) numbers. Updates have been made to reduce the duplicated logs.

Issue Identifier	Description
64076	When a template with the L3 Forwarding Enabled option selected was created on Panorama running a Panorama 5.1 release version, commits could not be performed after then upgrading to the Panorama to run PAN-OS 6.0.2. This was due to a migration issue that occurred during the upgrade and was related to the L3 Forwarding object. This issue is now resolved.
63854	Resolved an issue where a virtual systems administrator could not use the XML API to add IP address to username mappings.
63395	Custom reports configured on Panorama were not being pushed to a PA-7050, and were displaying on the PA-7050 with no data. This has issue has been resolved so that custom reports configured on Panorama are successfully pushed to a PA-7050 and display correctly.
62565	Resolved an issue where OSPFv3 was not redistributing a default route correctly.
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. The GoDaddy Root Certificate Authority - G2 has been added to the list of trusted CAs.
61038	Resolved an issue where the device server would sometimes fail to send a URL request to BrightCloud, and the URL categories would display as not resolved.
60030	URL Filtering logs now display when a search has been successfully blocked due to Safe Search Enforcement. An entry with a `block-url` action is listed in the URL Filtering logs whenever a user is presented with a block page (**Monitor > Logs > URL Filtering**).

PAN-OS 6.0.4 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.4 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

Issue Identifier	Description
66157	Fixed an issue on a PA-7050 firewall, where traffic through an IPSec tunnel failed during tunnel key renegotiation due to a race condition.
65643	When a firewall was configured with both 1GB and 10GB interfaces, and a 10GB interface went down, a back-end process was not reporting the link down event instantly. An update was made to prevent back-end processes from delaying to report an interface's link status as down.
65612	Fixed an issue that occurred when Panorama was running a PAN-OS 6.0 release version and a managed firewall was running a PAN-OS 5.0 release version. Reports generated for WildFire private cloud were not accessible on Panorama and showed the error message: `the requested resource does not exist.`
65557	In certain situations, a firewall in a high availability (HA) configuration could exit a suspended state without user intervention. With this fix, additional checks have been implemented to ensure that a firewall can exit a suspended state only due to an administrator request using the CLI or web interface.
65534	Resolved an issue that caused a PA-7050 to restart due to a link failure. This was due to an issue where when a link failure occurred, only one side of the link was being reset. Link detection has been updated so that if a link failure occurs, both sides of the link are reset.
65445	Addressed an issue where the ACC charts on the firewall web interface did not display any data after the order of the columns was modified and the width of the columns was adjusted.
65396	Fixed an issue that occurred when the option to **Share Unused Address and Service Objects with Devices** was disabled on Panorama. When this option was disabled, attempting to commit a Device Group to a managed firewall failed.
65328	Addressed an issue with Panorama where logs were not being uploaded. The use of a space character in Log Collector Group names led to this issue. You can no longer include a space character in a Log Collector Group name.
65316	The firewall web interface would allow you to add an **Exempt IP Address** to a vulnerability from the Threat Logs but did not save the settings and enforce the IP exception unless an **Exempt Profile** was also selected. The web interface has been updated so that you cannot add an **Exempt IP Address** without also selecting an **Exempt Profile**.
65278	Selecting a service object displayed in the Service column for a Security policy rule and then selecting **Value** did not expand to display the service object's members as expected (**Policies > Security**). This has been updated so that selecting a service object in the Service column correctly displays the service object's **Value** fields.
65156	A security-related fix was made to address CVE-2014-0224. For additional information, refer to PAN-SA-2014-0003 on the Security Advisories site (https://securityadvisories.paloaltonetworks.com).

Issue Identifier	Description
65146	Resolved an issue that occurred in a high availability (HA) active/active configuration, where HA3 packets could drop for a few seconds on the active-primary device while a content update was running on the active-secondary device.
65098	Resolved an issue that was seen after a shared policy was pushed from Panorama, where all traffic through a firewall stopped. This was due to an issue where the routing loop configuration between two Virtual Routers was causing incorrect programming to the offload processor on the PA-4000 Series firewall.
64960	In a high availability (HA) active/active configuration, when a device received Jumbo packets that had been fragmented, it transmitted the packets as fully assembled Jumbo packets. This issue has been resolved so that fragmented Jumbo packets are no longer transmitted as assembled Jumbo packets; both fragmented and assembled packets are transmitted correctly.
64870	Resolved an issue that was seen in a Panorama high availability (HA) active/passive configuration, where saving the configuration on the active device did not correctly sync the predefined configuration to the passive device.
64795	Custom application port settings were getting deleted inadvertently by clicking the **OK** button after opening the specific custom application. This issue has been addressed so that clicking the **OK** button after opening a custom application entry does not delete port settings.
64656	Addressed an issue that occurred on PA-3000 Series firewalls, where the dedicated HA2 port was taking more than 10 seconds to link up when an Ethernet cable was connected.
64591	The fix in this bug resolves two issues: • PA-3000 Series firewalls could stop passing traffic due to errors in the internal data path. A registry value was changed in the dataplane packet processor to prevent this error. • When highly compressed traffic is passing through PA-7050, PA-5000 Series, or PA-3000 Series firewalls, this caused some additional latency in other traffic passing through the firewall. This fix prevents the latency from being introduced to the traffic by changing the amount of data being handled by the signature matching FPGA.
64553	When using the PAN-OS integrated User-ID agent, after the mapping has timed out, the firewall continued to send WMI probes to devices that were no longer responding. With this fix, the firewall does not perform WMI probing after the time-to-live (TTL) timer for an IP address to username mapping expires.
64438	Static DNS proxy entries configured on the DNS Proxy page are set with an initial TTL value of 7 days. For static DNS proxy entries, the TTL counter should always remain at the initial value; however, in this case, the TTL counter for the static DNS proxy entries was counting down to zero. This issue has been resolved so that the TTL value for static DNS proxy entries remains at 7 days.
64322	Resolved an issue where Panorama was running a PAN-OS 6.0 release version and could not push Dynamic Address Groups to a firewall running a PAN-OS 5.0 release version. This issue has been resolved and was due to migration issues caused by the removal of the Dynamic Address Object functionality in PAN-OS 6.0.
64289	Addressed an issue where SSL Certificate Common Names containing uppercase characters were not parsed properly due to case sensitivity. In certain conditions, this caused the URL Categorization lookup to fail and the issue has been resolved.

Issue Identifier	Description
64166	After approximately 388 days of uptime, the firewall lost the IP address to username mappings on the dataplane. This issue has been addressed so that the firewall does not lose IP address to username mappings when it reaches this uptime.
64122	Addressed an issue where a User-ID process unexpectedly stopped on the passive device in a high availability (HA) active/passive configuration. This was due to an issue caused by a restart of the Windows server that was hosting the Terminal Server Agent.
63971	Addressed an issue where the Network File System (NFS) process failed intermittently on PA-5000 Series devices configured in a high availability (HA) configuration. This issue occurred because HA session updates were not being processed in the correct order and sessions were stalled. Though the issue was not specific to NFS traffic, it was more prevalent for NFS traffic and other application traffic with long session timeout periods.
63658	An update was made to support the export of threat packet capture (PCAP) files using the XML API for a role-based user.
63620	Fixed an issue with PA-3000 Series firewalls where traffic could stop passing through the firewall or the dataplane could restart due to errors seen on the field-programmable gate array (FPGA).
63423	Resolved an issue with the firewall web interface where attempting to filter traffic logs using the parameter `user in` caused the management plane to stop responding.
63304	A dataplane process stopped unexpectedly when processing malformed inbound-proxy SSL encrypted handshake packets. Defensive protection logic has been incorporated to gracefully handle these packets and to avoid process failures.
63113	Resolved an issue where MIB walk counters were showing different information than the output of the `show session info` command on the firewall.
63110	Changed the level of a User-ID log to show as a debug log instead of a warning log.
62741	The feature that allows you to configure polymorphic objects in the Panorama web interface was not working in PAN-OS 6.0 release versions (the feature worked as expected in PAN-OS 5.0 release versions). This feature allows you to configure objects that do not exist in policies on Panorama if the following command is configured: `debug skip-policy-address-check yes`. This issue has been fixed so that the polymorphic objects feature works correctly.
62410	With SSL decryption enabled on the firewall, certain web sites that use Transport Layer Security (TLS) Renegotiation were failing to load because the sites' certificates included renegotiation extensions. An update was made so that the firewall supports TLS Session Renegotiation.
62323	Made fixes to improve the issue where the firewall went into a non-functional state due to an out of memory condition caused by an internal process. Updates have been made to resolve some of the memory utilization issues.
62305	In a multiple virtual system environment, subsequent commit failures were seen following an upgrade to a PAN-OS 6.0 release version. This occurred when prior to the upgrade, Panorama had pushed security policies that reference tags. This issue has been resolved so that following an upgrade to PAN-OS 6.0.4 or later release version commits are successful and tag objects pushed from Panorama prior to the upgrade are automatically created.

Issue Identifier	Description
62244	When trying to add an address object to a policy, the search drop-down failed to display the configured address object. This issue was only seen when the number of address objects available exceeded 500 objects, and has been addressed so that address objects are displayed correctly when using the search drop-down to add the object to a policy.
61972	When highly compressed traffic passes through a PA-7050, PA-5000 Series, or PA-3000 Series firewall, this caused some additional latency in other traffic passing through the firewall. This fix prevents the latency from being introduced to the traffic by changing the amount of data being handled by the signature matching FPGA.
61846	The firewall web interface required the field **Peer HA1 IP Address** to be populated in order to disable high availability (HA). This has been addressed so that the field **Peer HA1 IP Address** is not mandatory to disable HA.
61170	The PAN-OS 6.0 SNMP MIB has been updated to add 42 new system log traps. The new traps are added as follows: • 5 traps added under PAN_ELOG_EVENT_HA • 3 traps added under PAN_ELOG_EVENT_VPN • 2 traps added under PAN_ELOG_EVENT_USERID • 11 traps added for PAN_ELOG_EVENT_MDM (new category) • 21 traps added for PAN_ELOG_EVENT_RAID (new category) • 2 traps added for PAN_ELOG_EVENT_VM (new category) You can download the updated SNMP MIB (PAN-MIB-MODULES-6.0-RevC.zip) from the following location: https://live.paloaltonetworks.com/docs/DOC-6587.
61641	Addressed an issue where incorrect entries and information were displayed when moving between pages in the **Monitor** tab on the web interface.
61632	Addressed an issue where a service route was configured for a syslog server using a destination IP address, but the syslog server's traffic was using the management port.
61329	Using the web interface to add an IP address to a security policy, where a subnet was added without a proper subnet mask (for example, `1.1.1.1/`), was not blocked as an error. The expected behavior would be to block adding an IP address ending with a / as that character could translate to a value of any on the dataplane. An update was made to check for the / character.
59795	For administrators that logged into the web interface using RADIUS authentication, configuration changes did not cause the **Commit** button to be lighted (the **Commit** button showed as disabled) and were not displayed on the **Device > Config Audit** page. This issue did not exist for administrators authenticating using the local database. This issue has been resolved for all authentication methods (local user database, RADIUS, and LDAP).
59715	On PA-5000 Series devices, when sessions were initiated on different dataplanes 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 destination NAT (DNAT) policy setup.
57687	An update was made to enhance initialization of the PAN-DB cloud lookup process during device startup.
56786	Security rules with a URL category attribute were not being correctly matched against certain sessions with `set deviceconfig setting ssl-decrypt url-proxy` enabled, which sets a proxy for SSL sessions if the URL category is blocked. An update has been made so that a security policy lookup is performed after the URL category is received for proxy purposes, in order to ensure the information is retrieved correctly.

Issue Identifier	Description
40883	Addressed a root partition that was at 100% usage due to an issue where FireMon processes (where FireMon was being used as an external third-party monitoring utility to the Palo Alto Networks firewall) continued to run on a device and did not close correctly, even after the FireMon connection had timed out.

PAN-OS 6.0.3 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.3 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

Issue Identifier	Description
63862	A back-end process was using an excessive amount of memory, causing an out of memory condition. An update has been made to improve how out of memory conditions are addressed. When an out of memory condition occurs, the back-end process will be terminated in place of any other critical processes. This ensures that any critical processes will continue to run despite an out of memory condition, and the back-end process will later restart automatically.
63859	A PA-500 device was not sending out scheduled email reports. This was due to a rare issue where report generation was suspended and a race condition caused it to be unable to resume, resulting in subsequent scheduled reports failing to generate. This issue has been addressed so that the report generation process is able to correctly resume after being suspended.
63635	Addressed an issue where Panorama restarted unexpectedly due to a back-end reporting process that stopped responding.
63626	The clear log operational command was not available on the PA-7050 firewall in the first three releases of PAN-OS 6.0 (6.0.0, 6.0.1, and 6.0.2). As of PAN-OS 6.0.3, this command is now available.
63608	Upgrading from a PAN-OS 5.0 release version to a PAN-OS 6.0 release version failed when the PAN-OS 5.0 configuration included a custom application configuration that included the spyware identification option (CLI command: `spyware-ident`). This was related to the spyware identification option not being supported in PAN-OS 6.0 release versions until PAN-OS 6.0.3. This issue has been addressed so that upgrading to PAN-OS 6.0.3 or higher release versions is successful, even when the PAN-OS 5.0 configuration includes a custom application configuration with the spyware identification option.
63602	An issue was resolved where a User-ID process on the firewall stopped working when a connected User-ID Agent sent an XML API logout message containing a valid IP address but no entry name.
63587	Custom signatures added as exceptions to a Vulnerability Protection Profile were not being displayed on the **Exceptions** tab on the Panorama web interface (**Objects > Vulnerability Protection > Exceptions**). This issue has been addressed so that custom signatures added as exceptions to a Vulnerability Protection profile are correctly displayed on the **Exceptions** tab.
63582	On the Panorama web interface, attempting to filter target devices to which specific security rules have been applied did not display results. This issue has been addressed so that the filter works correctly.
63570	Addressed a race condition that caused scheduled report generation to stall preventing scheduled reports from generating.

Issue Identifier	Description
63551	Selecting **Sync to Peer** on the **High Availability** widget on the web interface **Dashboard** did not display the expected pop-up to confirm the sync to peer. This issue and another minor display issue were seen using an Internet Explorer 9 or Internet Explorer 10 browser to use the web interface. These display issues have been addressed.
63472	Smart card authentication for GlobalProtect was displaying the following error message: `Authentication failed: empty password`. This issue has been addressed so that authentication is successful and the password field is correctly populated.
63422	Scheduled reports were not showing resolved host names. This was caused by an attribute value that was incorrectly set in one of the functions responsible for resolving the hostname for a given IP address. The value for this attribute has been corrected.
63383	Addressed an issue where DNS Proxy did not use the expected DNS server (according to the configured DNS Proxy rule) to perform a name server lookup.
63316	Addressed an issue that occurred when attempting to log in to the Panorama web interface. After authenticating login credentials and displaying the message: `Creating administrative session. Please wait…`, a white screen was displayed instead of the Panorama web interface **Dashboard**. This issue has been resolved so that logging in to the Panorama web interface correctly displays the **Dashboard**.
63298	Addressed an issue where syncing a configuration between Panorama high availability (HA) peers did not work correctly.
63282	Fixed an issue where a VM-Series firewall on a Citrix SDX server would not reboot into maintenance mode to allow administrators to perform specific tasks, such as reverting images or changing between FIPS and CC mode.
63247	During Session Initiation Protocol (SIP) registration, if there was no port specified in the SIP payload, the device did not add any NAT information to the SIP payload. This caused some SIP servers to use more aggressive registration intervals using the RTP Control Protocol (RTCP). This has been fixed by adding a new application: `sipviaheader-nat`. An Application Override policy is required to use this new application.
63242	A field-programmable gate array (FPGA) change was made to handle microbursts of multicast traffic and improve recovery mechanisms in latency conditions.
63161	Resolved an issue where the NetBIOS name was removed from the IP address to username mapping when the NetBIOS name contained a period punctuation mark.
63147	Fixed an issue in the migration script for the Routing Information Protocol (RIP) export rules from PAN-OS 5.0 release versions to PAN-OS 6.0 release versions that caused Panorama template commits to fail.
63106	Addressed an issue that affected an upgrade from a PAN-OS 5.0 release version to a PAN-OS 6.0 release version, where an IPSec validation error occurred when the dynamic peer type on an IKE gateway had the Local and Peer IDs defined.
63086	Resolved an issue that occurred in a high availability (HA) active/active configuration, where the parent application sessions on a HA peer were not updated with traffic from the child application session and the parent applications sessions timed out. This caused the parent applications to close on both devices in the HA pair. This has been updated so that when the parent application session is refreshed on the primary device, it is now also refreshed on the secondary device.

Issue Identifier	Description
63052	When attempting to connect to GlobalProtect with token-based authentication configured, and a token could not be found, different error messages were previously displayed depending on the GlobalProtect or PAN-OS release version. This error message has been updated to be consistent across release versions.
62995	Addressed an issue where the Application usage and Traffic summary by URL Category information in User Activity Reports was not in sync with the information displayed on the **ACC** tab in the web interface, in the **Top Applications** and **URL Filtering** sections.
62985	An issue with the FPGA code for some PA-3000 Series devices was causing a small amount of VLAN tagged and offloaded packets to be truncated by 4 bytes.
62969	Online Certificate Status Protocol (OCSP) requests were using the OCSP location in the certificate instead of the location configured on the firewall. This has been adjusted so that the OCSP configuration on the firewall will take precedence. If no OCSP location is configured on the firewall, the certificate OCSP location will be used.
62895	Addressed an issue where members of groups on non-Active Directory LDAP servers were not displayed as group members on the firewall.
62883	Addressed an issue where fiber port down detection on SFP ports on a PA-2000 Series device took 10 - 20 seconds.
62876	A Panorama role-based administrator with privileges for Device Groups and Templates could view devices which were not included in any device groups or templates. An update has been made in the web interface to eliminate visibility into devices that are not a part of a device group for administrators limited to Device Groups and Templates privileges.
62827	Addressed an upgrade schema issue for Panorama running PAN-OS 6.0.1 where address objects were causing commit errors when attempting to push a configuration from Panorama to managed devices.
62801	Traffic was blocked during SSL decryption when a certificate was signed with an untrusted CA and when the option to use OCSP to check certificate status was enabled (**Device > Setup > Session > Certificate Revocation Checking**). This has been resolved so that decryption works with untrusted certificates, with the option to use OCSP to check certificate status enabled.
62763	Group mapping queries failed if the group name, or Active Directory organizational unit (OU) path, contained characters that were used in the standard LDAP query syntax (for example, parenthesis). These characters were not escaped correctly during the query building process causing the query to fail. An update was made so that the special characters are escaped.
62663	Resolved an issue where the status for Tor was inaccurately reported in the outputs for the `show wildfire status` and `test wildfire tor` CLI commands.
62596	A shadow rule warning message was incorrectly displayed and was not accurate in indicating that a security rule's match criteria was met by a preceding rule (the match criteria had not been met by a preceding rule). The incorrect error messages were being displayed while performing a commit and a fix was made to eliminate the incorrect warning messages.

Issue Identifier	Description
62595	Addressed an issue that was seen when using a filter to define search criteria for WildFire logs on the web interface. When adding a log filter for WildFire logs, selecting Category as the Attribute to include in the search displayed URL categories to select from in the **Value** column (**Monitor > Wildfire > Add Log Filter**). The **Value** column should have only displayed the options Malicious or Benign to select from.
62591	During extremely high rates of logging over an extended period of time, traffic and threat logs could not be displayed on the web interface or the CLI. This was due to the dataplane logging process consuming too much memory when attempting to write very large amounts of traffic logs and has been resolved.
62586	When upgrading Panorama, commits to device groups would fail if Panorama had Service Groups and Address Groups configured with the same name. This has been resolved so that group objects are independent and unique names are not required.
62573	Fixed an issue where upgrading a VM-Series firewall with the VM-1000-HV license caused a firewall to go into maintenance mode without any indication of why it did so. This issue occurred because the VM-1000-HV license requires 5GB RAM to support higher capacities but, prior to PAN-OS 6.0.3, the memory requirement was not enforced, making it possible to apply the VM-1000-HV license to a VM-Series firewall without enough memory allocated (default allocated memory is 4GB). With this fix, a memory requirement check is added so that the VM-Series firewall will boot to maintenance mode with an error informing you that you need to increase the allocated memory on the firewall to 5GB or more.
62559	Resolved an issue where creating or modifying policy rules took a long time for large configurations (for example, a configuration with 3000 rules and 20,000 objects). An update was made to increase the speed for creating and modifying policy rules for large configurations.
62552	With both SSL Inbound Inspection and virus scanning enabled, the firewall was able to detect a virus being sent, but did not block the virus from being forwarded to the target. With this fix, the virus file is not forwarded to the target.
62545	An update was made to support the export of threat packet capture (PCAP) files using the XML API.
62391	When displaying the Detailed Log View of a traffic log entry, the value of the attribute **Receive Time** was incorrect and did not match the value from the **Receive Time** column on the traffic log list. With this fix, the value of the **Receive Time** attribute in the Detailed Log View is shown correctly.
62377	Following an upgrade to PAN-OS 6.0.1, the following unexpected system log was generated daily: `Got batch event for unknown child acc_rollup`. An update has been made so that the log is no longer generated daily.
62366	The dataplane restarted with multiple cores due to a race condition caused by updating the aged out session. This issue has been fixed so that the race condition is resolved and will no longer trigger a restart.
62315	Resolved an issue for devices running PAN-OS 5.0 or PAN-OS 6.0 release versions, where the disk quota displayed on the Panorama web interface for a Log Collector group was not reflective of the actual disk quota output.

Issue Identifier	Description
62291	An issue was occurring where any type of commit triggered the `syslog-ng` configuration to be reloaded and the connection to be reset. This issue was fixed so that only commits related to the syslog server configurations and syslog-related log forwarding configurations will trigger a `syslog-ng` configuration reload and the connection to be reset.
62219	Unexpected XML data was present when loading an existing configuration version from the device. This resulted in a commit failure that cited the unexpected text. An update has been made to avoid this condition and to ensure a successful commit when loading an existing configuration version.
62179	In certain situations, a tunnel interface appeared to be up and was present in the forwarding table, although the underlying IPSec tunnel was down. This issue occurred when the IPSec tunnel had a VPN Monitor profile configured with Fail Over enabled, and the device was restarted while the remote IPSec endpoint was down. With this fix, the status of the tunnel interface matches the state of its corresponding IPSec tunnel when a VPN Monitor profile with Fail Over enabled is configured, and regardless of the initial state of the tunnel.
62113	Resolved an issue for a PA-7050 device, where TAP Mode traffic did not load balance properly on a Network Processing Card (NPC), and caused a much higher load on one dataplane in comparison to another dataplane.
61987	Resolved an issue where virtual firewalls running PAN-OS 6.0 release versions did not correctly sinkhole suspicious DNS queries.
61953	When the IPv6 address `::/0` was configured under the Permitted IP Addresses section in an Interface Management profile, IPv6 communication to the interface was not allowed. Since IPv6 address `::/0` is equivalent to `any`, IPv6 communication should be allowed from any IPv6 host. This has been addressed so that you can add the IPv6 address `::/0` under Permitted IP Addresses for an Interface Management Profile to successfully allow IPv6 communication from any IPv6 host.
61879	IPSec VPN traffic could not be initiated following a restart of the `sysd` process. This issue has been resolved so that IPSec VPN traffic can be initiated even if `sysd` process is restarted.
61864	Fixed an issue where a PA-5000 Series firewall was dropping Skinny Call Control Protocol (SCCP) traffic after an upgrade to PAN-OS 6.0.0; SCCP sessions were timing out within 5 seconds due to communication issues between dataplanes. With this fix, the parent session timeout value is set appropriately and SCCP traffic is not dropped.
61855	Resolved an issue where multiple configuration pushes from Panorama to a managed device could cause that managed device's management server to restart. When this occurred, a system log would be indicating that the management server was restarted due to high memory utilization. This issue is resolved so that commits from Panorama to managed devices succeed for multiple configuration pushes and the management server remains stable.
61827	Addressed an issue where a virtual wire with **Link State Pass Through** enabled had one interface that remained connected despite the other interface being physically disconnected.
61785	Resolved an issue where an administrator for a single virtual system could delete logs for other virtual systems using the CLI.

Issue Identifier	Description
61781	Resolved an issue that occurred when using the Panorama web interface to set up SNMPv3 with a view. Adding a **View** with a space in the view's name caused SNMP polling to fail. This has been resolved so that an error is displayed if a space is used when naming a **View** and a new name can be entered without a space (**Panorama > Setup > Operations > Miscellaneous > SNMP Setup > Views**).
61757	The `show arp management` command timed out after 30 seconds without returning output if both primary and secondary DNS servers configured on the firewall were unreachable. The timeout has been increased up to 120 seconds to return ARP entries with or without DNS resolved names. The time taken to return the output could vary based on the number of DNS servers configured and the availability of the DNS servers to resolve host names.
61724	When a custom report was exported to CSV format, the device name in the report was showing the device's serial number instead of the device name. This has been fixed so that exporting a custom report to CSV format correctly shows the device name in the device column.
61643	Resolved an issue where email alerts were displaying all values on a single line. This occurred when the email alerts were based on custom log formats that were configured with a `\n` or a new line as a separator between fields.
61350	Following an import of a license key file from the CLI, several checks were performed to verify the certificates validity and an error was seen where the file size of the key file could be misinterpreted and the file incorrectly rejected. This issue has been resolved so that importing a valid license key file is successful.
61329	Using the web interface to add a an IP address to a security policy, where a subnet was added without a proper subnet mask (for example, `1.1.1.1/`), was not blocked as an error. The expected behavior would be to block adding an IP address ending with a / as that character could translate to a value of any on the dataplane. An update was made to check for the / character.
61326	Addressed an issue that occurred in a high availability (HA) configuration, where link monitoring for a 10G port displayed the wrong status for the port when the port was down.
61284	Traffic using policy-based forwarding (PBF) with symmetric return enforced experienced packet loss due to failed return MAC address lookups. This issue was caused by another change made in PAN-OS 5.0.11 which changed the PBF return MAC learning from the forwarding state to the session start; the PAN-OS 5.0.11 change that caused this issue has been reversed, which fixes the issue.
61276	Resolved an issue that occurred while replacing a device following an RMA. After issuing the `replace device` CLI command, exporting the device state did not show the appropriate configuration fields to set up the replacement device.
61254	H.323 video calls were getting dropped intermittently when video call traffic was creating a multi-level application-level gateway (ALG) session dependency pattern. The issue was observed when the grandparent session had a low timeout value and then timed out, causing its dependent parent and grandchild sessions to be terminated and the video call was dropped. This has been addressed so that TTL counters of both parent and grandparent sessions refresh and do not time out while the corresponding grandchild session continues to see traffic.
61101	Resolved an issue where the Address Resolution Protocol (ARP) table was not updated following Spanning Tree Protocol (STP) re-convergence in the network.

Issue Identifier	Description
61058	Resolved an issue that occurred when a NAT Policy rule was configured to use a Dynamic IP pool for IP NAT translations and a fall back pool was also configured to perform **Fall Back Dynamic IP Translation** if the Dynamic IP pool ran out of addresses. In certain cases, the fall back pool was being used for translations when the IP pool was not exhausted.
60781	A Dynamic Block List address object (0.0.0.0) was being added to security rules where that Dynamic Block List was referenced, even though that object did not exist in the Dynamic Block List source file. This was due to issues with EBL Refresh, and has been addressed so that when a Dynamic Block List is referenced in a security policy, the Dynamic Block List objects displayed in the policy are accurate.
60634	Inter-vsys multicast traffic caused the dataplane to restart. The restart was due to a fragmented packet that was encapsulated into a Protocol Independent Multicast (PIM) packet and routed to another virtual system. The fix prevents this kind of fragmentation of the packets.
59852	Fixed a high dataplane CPU usage issue seen on PA-5000 Series devices that was caused by FPGA lock-up.
59331	Syncing a high availability (HA) configuration failed. This occurred when the MTU size on the management interface was set to a value smaller than the default MTU size, and dataplane interfaces were using the MTU size value set on the management interface. This resulted in dataplane interfaces (in this case, including the HA interfaces) to drop packets that were larger than the MTU size set on the management interface.

PAN-OS 6.0.2 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.2 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

Issue Identifier	Description
62578	A Panorama administrator with privileges to manage Device Groups and Templates was unable to perform management and administrative functions due to several buttons and functionalities appearing to be disabled on the web interface. The issue has been resolved so that a Device Groups and Templates admin can successfully perform management and administrative functions as defined by the admin role.
62567	An issue was addressed where commits were failing intermittently following an upgrade to PAN-OS 6.0.1. This was due to the management server failing to send the ID request to the client device and has been fixed so that commits are successful following an upgrade. A second issue was addressed with this fix, where high availability (HA) synchronization was showing an error message when there was no URL Filtering license; this occurred when the PAN-DB cache was empty and the passive device treated the empty files as corrupt files.
62386	The URL category match within a security policy was not enforced, allowing non-HTTP traffic to match the rule. This update ensures proper enforcement of the URL category selection in a security policy.
62352	Addressed an issue where templates pushed from Panorama were missing BrightCloud to PAN-DB conversion files, resulting in errors when managed devices attempted to translate URL filtering policies pushed from Panorama.
62321	The Panorama web interface was inaccessible due to a corruption in MongoDB journal files. A fix was made so that if a MongoDB journal file becomes corrupt, Panorama now recovers correctly by removing the journal files and then recreating them.
62244	When trying to add an address object to a policy, the search field failed to return the address object. This issue was only seen when the number of address objects available exceeded 500 objects.
62218	Fixed an issue where an administrator with full privileges on Panorama could not delete most of the configuration on the **Network** tab of the Panorama web interface. This issue has been addressed so that all objects on the **Network** tab can be created, modified, and deleted.
62208	Resolved an issue where service routes for email alerts and SNMP messages did not take precedence if the management interface was disconnected.
62199	Panorama failed to commit when attempting to push a configuration to a managed device. This occurred when the pushed configuration included a decryption profile; even though there were no decryption port mirroring options selected in the decryption profile, the managed device did not support decryption port mirroring and the commit failed. This was due to Panorama not pruning out the portion of the configuration that was specific to decryption port mirroring and has been fixed to ensure that configuration parameters are removed when pushed to devices that do not support them.
62084	Addressed an issue where domain names greater than 63 characters were getting truncated in the resolv.conf file for Linux and Mac OS even when separated by commas.

Issue Identifier	Description
62076	After creating an Anti-Spyware profile with the **Action on DNS queries** set to **Block** (**Objects > Security Profiles > Anti-Spyware > Anti-Spyware Profile > DNS Signatures**), the threat logs for a suspicious DNS query displayed the action taken on the threat traffic as `reset-both`. This has been updated so that when the action is set to **Block** for DNS queries in an Anti-Spyware profile, the threat logs will show the action taken on the suspicious DNS traffic as `drop-all-packets` when using UDP (the threat logs will still show the action taken on suspicious DNS traffic as `reset-both` when using TCP).
62057	FTP log export failed when an explicit destination path was defined. In cases where multiple CSV files were used, the first CSV file was created but subsequent CSV files failed. This was updated to allow the creation of multiple CSV files during file export.
62020	When a device is configured to use a Time Zone with a name that is abbreviated to more than three characters (for example, America/Anchorage abbreviated to AKST), the web interface displayed an error message on the Dynamic Updates page. This issue did not affect already configured automatic updates. Workarounds for this issue include using the CLI to configure and view dynamic updates and re-setting the Time Zone of the device to a Time Zone with a name that is three characters or less, for example, America/Los Angeles abbreviated to PST. This issue has been addressed so that the Time Zone and the corresponding Time Zone name the device is configured to use do not cause an error on the Dynamic Updates page.
61985	The GlobalProtect portal became inaccessible using the web interface or the GlobalProtect client after an interface address change. This normally occurred when an interface was DHCP enabled and an address renewal occurred. The issue was caused by an address map change which published incorrect interface data to the SSL VPN component. The address map change operation has been corrected to publish the correct data.
61951	SSL Inbound Inspection sometimes failed due to SSL session reuse. This issue has been resolved so that SSL Inbound Inspection is successfully enforced according to the configured decryption policy.
61992	PA-4000 Series firewalls running PAN-OS 6.0 in a high availability (HA) active/active configurations utilizing Virtual or Floating IP addresses experienced intermittent connectivity. (HA active/passive configurations on PA-4000 Series firewalls running PAN-OS 6.0 releases were not affected by this issue.) Workaround (limited): Configure static ARP entries that are bound to the physical interfaces; however, this creates the possibility of losing failover capabilities in HA active/active configurations and force traffic to prefer one firewall over another.
61897	The following error message displayed when loading Enterprise 6.0 SNMP MIBs using the ManageEngine SNMP MIB Browser: `Could not parse the file PAN-COMMON-MIB. Couldn't resolve these sequence constructs`. This issue has been resolved by fixing capitalization errors on the MIBs.
61844	Under extremely heavy load with fully Layer 7 traffic, the PA-7050 firewall was experiencing packet loss due to the depletion of the software buffer.
61840	Auth and priv passwords for SNMPV3 setup on managed collector groups were displayed in clear text. With this fix, the passwords are masked and are not shown in clear text.
61828	TCP SYN cookies were activated sooner than the **Activate Rate** set in the DoS protection profile. Using DoS Protection with SYN cookies now activates correctly according to the configured SYN count.
61747	The use of a 64-character string as a RADIUS shared secret was not supported. A fix is implemented to ensure a higher value for the buffer to store and encode shared secrets.

Issue Identifier	Description
61742	With safe search enabled, when a user was attempting to access a regional site (for example, www.google.co.uk), a block page appeared directing the user to update the preferences page for the main site and not the regional site (for example, the block page directed the user to google.com preferences instead of www.google.co.uk). However, updating the preferences page for the main site did not enforce the preferences on the regional site. This has been fixed so that block pages display the correct preferences page for regional sites.
61714	Traffic logs were not displayed on a PA-7050 firewall despite traffic being generated. This was due to a disk failure and there was no system log was generated for the disk failure. This has been addressed so that a system log is generated to notify if disk failure event occurs during raid rebuilding.
61696	When using SSL Forward Proxy decryption with self-signed certificates with Firefox, an error was seen from Firefox regarding conflicting certificate serial numbers: `sec_error_reused_issuer_and_serial`.
61683	Fixed an issue with configuring SNMPv3, where an SNMPv3 user with a view could not be added. An error was displayed when attempting to add a name for a view, where the error message stated that view is not a valid reference and the SNMPv3 user with a view could not be added (**Panorama > Collector Groups > Collector Group > Monitoring > Views**).
61682	An M-100 appliance failed to mount the file system for a RAID Disk Pair. There was no system log generated for this mount failure, and disks were shown as `Available`. This issue has been addressed so that a system log is generated when a disk mount fails, and disk is not made `Available`.
61675	After creating a Log Forwarding profile using the Panorama web interface (**Device Groups > Objects > Log Forwarding**), the Log Forwarding object always defaulted to being shared across device groups, regardless of whether the **Shared** checkbox had been selected when creating the profile. This has been fixed so that only Log Forwarding objects with **Shared** selected are shared across device groups. Log Forwarding objects where **Shared** is not selected correctly belong only to the Device Group displayed in the Device Group drop-down.
61579	When session offload is disabled, the sequence and acknowledgment (SEQ/ACK) number check dropped ACK packets. This was due to an issue with the sequence and acknowledgment number check and has been fixed. The workaround for releases prior to PAN-OS 6.0.2 is to use the `set deviceconfig setting tcp asymmetric-path bypass` command.
61471	Following a restart, an internal path monitoring failure that showed a false positive triggered a second dataplane restart. This issue has been addressed so that when the dataplane restarts, path monitoring stops and a false positive is not generated so that a second dataplane restart does not occur after reboot.
61437	On a few occasions, a device stopped authenticating any users. This was due to an issue where bind errors were causing an LDAP file descriptor leak and the issue has been resolved.
61396	When read using SNMP, the value returned for Dataplane CPU utilization was always zero. This was fixed so that the value returned for dataplane CPU utilization matches the true CPU utilization.
61387	Data connection of FTP in passive mode sometimes failed on PA-5000 Series devices. This has been fixed so that data connection of FTP in passive mode does not fail.

Issue Identifier	Description
61366	When loading a report template, the selected time period was being reset automatically. A fix has been implemented to limit this behavior.
61236	An issue was resolved to prevent the OSPF MD5 sequence number from resetting during a high availability (HA) failover or routed restart. Before this fix, there was a reset when a failover occurred. This reset caused a longer outage than expected. When upgrading from an earlier PAN-OS 6.0 release version to PAN-OS 6.0.2, allow a five minute grace period before a HA failover or routed restart. Following the five minute grace period, this limitation will not apply to further failovers or upgrades.
61174	Fixed an issue where license retrieval on the device was failing when the option **Verify Update Server Identity** was enabled on the **Device > Setup > Services** page.
61168	SYN packets were dropped when a session with the same 5-tuple (same source IP address, destination IP address, source port number, destination port number, and protocol) is received by the firewall at the same time the existing session gets aged-out based on the TIME-WAIT period when source NAT (Dynamic-ip-and-port) was used.
61083	When using URL Filtering with `ssl-decrypt url-proxy` enabled, the block page failed to display on some browsers using SNI (Server Name Indication) because the firewall failed to retrieve the hostname from the SSL session in order to run decryption. With this fix, the process was improved to retrieve this information correctly.
60985	Fixed an issue with PA-3000 Series devices where traffic could stop passing through the firewall or the dataplane could restart due to an internal path monitoring failure.
60974	When a colon was used in password field to generate an API key, using that API key displayed the error `Invalid Credentials`. The way that passwords are handled has been updated to allow a colon as part of the API key.
60928	In certain situations on the Global Protect gateway, the context for an IPSec tunnel to a GlobalProtect client showed the presence of NAT-T, although there is no NAT between the client and the gateway. Traffic through that IPSec tunnel failed. This issue was caused when a tunnel context ID previously used for a tunnel with NAT-T was re-used for a tunnel without NAT-T. With this fix, tunnel contexts are properly cleared before re-use.
60902	An issue was resolved where subinterface names with length greater than 16 characters were being truncated in the output of some CLI commands, corresponding web interface sections, and system logs.
60743	An untagged subinterface caused stale hardware sessions on a PA-5000 Series device, and traffic failed when a new session was hitting the stale 5 tuple session. This issue has been fixed so that hardware session info is deleted when sessions are closed.
60673	LDAP groups containing non-ASCII characters in their names could not be processed by the firewall. Policies filtering on these groups were not working properly. With this fix, groups are received by the firewall, regardless of the types of characters used in their names.
60617	TCP connectivity issues occurred on a virtual machine when SYN Flood protection was enabled with SYN Cookies with the **Activate Rate** set to 0. This was related to an issue where active and passive FTP were not working under different NAT configurations and has been addressed so that both active and passive FTP work correctly under different NAT configurations and do not cause TCP connectivity issues. A workaround for this issue is to set the **Activate Rate** parameter for SYN Flood settings to a value greater than 0 (**Objects > DoS Protection > Flood Protection > SYN Flood**).

Issue Identifier	Description
60299	Multicast ICMPv6 traffic was causing a restart after enabling and disabling zone protection profiles multiple times.
60250	Logging into the Panorama web interface only displayed a blank gray page instead of the Panorama **Dashboard**. This issue has been addressed so that logging into the Panorama web interface correctly displays the Panorama web interface **Dashboard** and management functions.
60036	Addressed an issue in summary PDF reports where if the **srcuser** field is not in the format of `domain\username`, the **srcuser** field was left empty.
59542	When sessions were initiated on different dataplanes in a multi-vsys environment, session traffic failed to span across virtual systems. This issue has been resolved so that inter-vsys sessions succeed with a DNAT policy setup.
59289	An issue has been addressed where dataplane restarts were seen due to PAN-DB becoming unresponsive. New URLs could not be learned and the repeated attempts built up the URL cache and caused an excessive consumption of system resources, making the dataplane unstable.
57736	Active FTP through NAT (dynamic ip-port) did not work on a virtual machine. This issue has been addressed so that both active and passive FTP work under different NAT configurations.
57600	Resolved a display issue on the **Monitor > Logs > Configuration** page, where the IPSec pre-shared key was displayed in clear text format in the **After Change** column. The IPSec pre-shared key is no longer displayed in clear text in the Configuration Logs.
57599	Addressed an issue where the firewall was dropping ARP unicast packets which resulted in incomplete ARP entries and Layer 3 forwarding issues.
57412	Addressed an issue where User Activity Reports were sometimes not returning any results due to malformed XML output.
50798	Device fans running at lower speeds were sometimes causing a thermal alarm. This occurred when the dataplane restarted while the device was in a temperature alarm state. In this case, the fan's speed control value was set to the default value, causing the fan to run at the incorrect speed. This issue has been addressed so that the fan speed is recalculated based on the device's current temperature following a dataplane restart.
50091	Management plane services were not performing optimally during peak traffic periods. The size of the ARP table on the management plane was increased to address this issue.
48758	In some cases, large amounts of compressed HTTP traffic could cause the zip buffer to fill and it would not continue to process additional compressed HTTP traffic. Offload of compressed HTTP traffic now works correctly so that even large amounts of compressed HTTP traffic are processed by the zip buffer.
40883	Addressed a root partition that was at 100% usage due to an issue where FireMon processes (where FireMon was being used as an external third party monitoring utility to the Palo Alto Networks firewall) continued to run on a device and did not close correctly, even after the FireMon connection had timed out.
24804	When specifying a default route of 0.0.0.0/0 in an OSPF export rule, the route was advertised with a metric of 255. This was because there was no option to specify a metric when specifying a route in an OSPF export rule. This change removes the metric field from the redistribution profiles, and adds it to the OSPF export rule configuration.

PAN-OS 6.0.1 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.1 release. For new features introduced in PAN-OS 6.0, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

Issue Identifier	Issue Description
61193	A certificate chain error was causing commit failures due to an IKE code change in 6.0.0. The fix changes the error that causes the commit to fail to a warning so that the commit can be successful.
61004	Addressed an issue where a user in a custom admin role could only view HIP match logs but was unable to view log details. Clicking the spyglass icon on the web interface opened the **Detailed Log View**, but no information was displayed.
60971	Following an upgrade to PAN-OS 6.0.0, scheduled Dynamic Updates failed to be pushed from Panorama to managed devices.
60826	Issues relating to Tags with brackets were occurring after upgrading to PAN-OS 6.0.0, and Tags with brackets could not be created, edited or deleted. In PAN-OS 6.0.1, the brackets in existing Tags are replaced with quotes and new Tags that you create cannot include brackets.
60816	Following an upgrade to PAN-OS 6.0.0, syslog connection status warnings for all defined syslog connections appeared in the system log every hour and were categorized as critical. This was caused by a scheduled hourly rotation of the syslog-ng log file, during which the syslog-ng daemon would restart. This issue has been fixed by adding a condition to the log file rotation process requiring the log file to be 10 MB or more and the connection status warning will only be seen once every few months.
60780	On PA-5000 Series firewalls, restarts were seen under heavy load conditions and were due to an internal path monitoring failure. Enhancements have been made to avoid such restarts.
60700	1GB copper SFP interfaces belonging to an Aggregate Group would sometimes show the link status as down after a reboot of the firewall.
60677	Group mapping queries failed when nested groups with long group names were searched. The search queries showed group members to be missing. This was due to the query string (groups/nested groups) being truncated at 39 characters.
60650	When using the web interface to configure SNMPv3 on a high availability (HA) pair, the **EngineID** field should be optional; however, the **OK** button could be clicked when this field was blank. This has been fixed so that the **EngineID** field is optional.
60564	On Panorama, a system log message was generated when a log file used for internal processing was truncated. This system log message is not relevant for the administrator and will not be displayed in the system log.
60510	An attempt to revoke SSL certificates generated on Panorama failed. The issue was caused by an internal verification check failure involving shared certificate objects used in device groups that included firewalls enabled for multiple virtual systems. The verification check has been corrected.

Issue Identifier	Issue Description
60505	SYN packets were dropped if a session with the same source and destination IP addresses and port and IP protocols comes to existing session at the timing of aged-out TIME-WAIT period.
60502	On the Panorama web interface **Monitor**, the maximum number of pages displayed for logs is not consistent depending on the log numbers displayed per page.
60412	The user was unable to modify custom logo due to an unrecognized `mime-type` option (`Device > Setup > Operations > Custom Logos`).
60347	Some service route settings could not be configured when the web interface was set to a language other than English.
60337	Fixed an issue where XML API showed empty hardware counters for `show interface dedicated-ha1`.
60274	Fixed an issue where the XML API showed an error when running the `show -availability interface ha1` command using the rest API.
60255	On occasion, the web interface for the Citrix SDX server fails to execute a reboot or shutdown of the VM-Series firewall. To trigger a reboot or shutdown, use the Force Shutdown or Force Reboot options on the SDX web interface. If you need to modify the instance of the VM-Series firewall, make the changes while the instance is shutdown, and then power it on.
60225	Fixed an issue where the XML API showed an error when running show session rematch using the rest API.
60201	In a high availability (HA) active/active configuration, an IPSec key renegotiation timing issue caused the new IPSec session to be set to DISCARD until the next key renegotiation. This caused traffic loss until the next tunnel key renegotiation.
60189	When high availability (HA) active/passive peers lost communication on HA1 and HA2 links, a race condition caused the dataplane to restart.
60070	In order for Android devices to be able to connect to the Mobile Security Manager's device check-in for enrollment and subsequent check-ins, the Root CA certificate had to be used to sign the server certificate for the device check-in interface in the portal configuration that was being delivered to Android devices. This applied even if you purchased a server certificate from a well-known, trusted CA as recommended. This was because the GlobalProtect Android app does not look in its system store for certificate verification With this fix, GlobalProtect Android app will first look in its system store for certificate verification. If this fails, the app will proceed to verify certificates against the CAs from the portal configuration.
60063	SSL decryption with Internet Explorer was inconsistent with certificate common names, resulting in name mismatch errors for some sites.
60035	When an external zone was configured with a Zone Protection profile applied to it, large IPv6 packets were causing dataplane processes to fail when sent through the zone.
60012	Addressed issues that were causing filtering on the web interface to return incorrect results.
60011	When a User ID Agent Setup template was pushed from Panorama to a managed device, the application content updates were not available for viewing or cloning in the syslog filters list in the web interface (**Device > User Identification > User Mapping > User ID Agent Setup > Syslog Filters**).

Issue Identifier	Issue Description
59991	In a shared gateway setup, when the firewall was configured to drop inbound Destination NATed traffic for a particular application, the traffic logs for Destination NATed traffic to be dropped showed the post-translated address instead of the pre-translated address. This issue was fixed by displaying the original source IP address in the traffic logs instead of the translated IP address.
59989	The Panorama web interface was not displaying data on the **Monitor > Logs > WildFire Submissions** page. A query for the data with no filters continued loading for a significant amount of time and then eventually timed out. This was due to threat logs that were not handled correctly by Panorama running PAN-OS 6.0.0 when received from log collectors running releases previous to PAN-OS 6.0.0.
59973	For Android devices that were being managed by the GlobalProtect Mobile Security Manager, when authenticating to the GlobalProtect gateway using client certificate authentication, the GlobalProtect app for Android did not look up the identity certificate issued to the device during enrollment. Identity certificates were therefore not being used for gateway authentication as expected. This has been fixed so that Android devices are able to use identity certificates for gateway authentication.
59967	When the firewall was configured as a GlobalProtect satellite and was receiving access routes from another firewall configured as the GlobalProtect gateway, the routing resource counter for static routes was not incrementing or decrementing correctly. This behavior caused the maximum number of routes to be artificially reached and the firewall stopped accepting routing updates. The fix for this issue readjusts the counters for static routes and total routes when creating a redundant static route or deleting a non-existent one.
59915	The filter field on the **Policies > Security** page of the web interface returned different results when strings with the same value, but different patterns were entered. For example, xx.xx.xx.0-24 is an address object name which includes the IP/netmask pattern xx.xx.xx.0/24. Entering either string in the filter should return the same search results but one query was showing fewer results than the other.
59890	When a PA-4050 firewall reached the limit for max supported concurrent decrypted sessions, the dataplane restarted. A fix was added to ensure that device will stop decrypting sessions once the limit is reached and a restart will not occur.
59873	A TCP session could not be established when SYN Cookies was enabled and when both Aggregate and Classified DoS Protection Profiles were configured.
59772	Traffic logs from log collectors were not visible on the Panorama web interface.
59707	NTP information on the firewall was displayed in way that could lead to confusion; for example, stating that the server the device is synced with is not connected (connected: false). NTP information is now displayed more clearly (**Device > Setup > Services**).
59574	Fixed an issue where an Antivirus profile on Internet Explorer and Firefox browsers was not showing the default action in parenthesis (alert/drop/) for the decoders.
59471	Resolved an issue with registering dynamic tags on the VM-Series firewall. The VM-Series firewall did not allow you to register dynamic tags that included the single quote (') character.
59343	When a security policy was configured that did not have a URL Filtering profile applied to it, URL Filtering logs were still being generated and were visible on the **Monitor > URL Filtering** page.

Issue Identifier	Issue Description
59309	User Activity Reports were showing inconsistent results. This was due to the User Activity Report generation taking too long and timing out. The timeout for User Activity Report generation has been extended so that requested reports will run until all data is completely gathered.
59276	Fixed an issue where botnet reports failed to use URL Filtering data for report generation.
59256	Performing an SCP import of the logdb file failed with the error: `failed to verify for logdb import`.
59180	Session setup between a client and server was not completed in a high availability (HA) active/active configuration when configured with multi-vsys and multi-VR. The client from one virtual system could not reach the server located on a second virtual system because the session in the second virtual system was not set up correctly.
59126	In a high availability (HA) active/passive configuration, OSPF and BGP neighbors went down on an active device after the passive device unexpectedly restarted.
59031	When admin users tried to login to the CLI without previously logging into the web interface and there was a RADIUS authentication profile configured, the firewall sent out a request to the RADIUS server with an invalid password that was different from the one submitted by the user. This resulted in valid users being unable to authenticate to the RADIUS server.
59018	A network outage occurred when the number of active sessions reached 100,000 sessions. This occurred on a PA-3000 Series firewall and Detector Threats have been increased on PA-3000 Series firewalls in order to address this issue.
58971	The CLI output for the `show routing protocol bgp loc-rib-detail` command displayed the community field incorrectly when certain prefix combinations appeared in the IP addresses of the BGP neighbors.
58736	WildFire email notifications did not contain a date header.
58586	Fixed the inability to log into the Panorama web interface. This issue occurred because root partition on an M-100 appliance was at 100% usage due to old reports being incorrectly stored in the /tmp directory.
58268	Traffic was sometimes blocked during SSL decryption when the option **Use OCSP to check certificate status** was enabled.
58215	The output of the `show routing protocol ospf area` CLI command was updated to provide greater clarity for the values defined.
58212	New virtual systems could not be added after applying a virtual systems license and could only be added after restarting the management server.
57997	In a high availability (HA) active/active configuration, the User-ID agent status was displayed as `connected` on the active-secondary device. This issue has been addressed and the active-secondary device will only show a User-ID agent status of `disconnected` as only the active-primary device connects to the User-ID servers.
57660	The management ports on a PA-2000 Series firewall did not link-up when connected directly using a straight or crossover cable.
57601	Fixed an issue where Data Filtering logs were showing incorrect file names when the data pattern was matched against the files.

Issue Identifier	Issue Description
57261	A denied session was logged with the Action displayed as `Allow`. This occurred when the application denied was on port 80 and triggered the Captive Portal redirect.
56905	When a PA-5000 Series firewall received more than 3000 BGP prefixes, the web interface showed an error (`op command for client routed timed out`) when displaying the Local RIB for BGP. Also, when executing the `show routing protocol bgp loc-rib-detail` command, the CLI returned an error (`Server error : op command for client routed timed out`).
55318	The following commit warning message is now included when nested wildcards are used in a URL Filtering configuration: `Warning: Nested wildcards (*) in URLs may severely impact performance. It is recommended to use a single wildcard to cover multiple tokens or a caret (^) to target a single token.`
50932	In a high availability (HA) active/passive configuration, `seed` was removed from the `PAN-DB sync seed with HA` message because `MP cache` is what is synchronized instead of `seed`. Also fixed an issue where the synchronized `MP cache` is not loaded on the passive device.
47642	Logs were not being written to disk because the configuration on the Managed Collector and Collector Group was set up before the Managed Collector established a connection to Panorama. This has been fixed so that Panorama allows you to configure the Collector Group only after the Managed Collector has connected at least once. This allows Panorama to verify the availability of the disk(s) and its size, ensuring that logs are written properly to disk.
45529	In some User-ID implementations, server session reads picked up capitalized special characters, such as Ü. All capital letters should be set to lower case but this operation was not supported for special characters, which caused a mismatch between group mapping and user mapping.
41347	Packet capture (PCAP) filters were not filtering information accurately. This fix ensures that the PCAP filters match the criteria defined on the device and accurately capture all relevant frames in the session.

PAN-OS 6.0.0 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS® 6.0.0 release. For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 6.0.

Issue Identifier	Issue Description
60347	Some service route settings could not be configured when the web interface was set to a language other than English.
59772	Traffic logs from log collectors are not visible on the Panorama web interface.
59707	NTP information on the firewall was displayed in way that could lead to confusion; for example, stating that the server the device is synced with is not connected (connected: false). NTP information is now displayed more clearly.
59407	NetFlow (type 4) messages were appearing in the traffic log database and reports.
59128	After logging in to Panorama using the CLI with RADIUS credentials, the following error message was printed: `Server error : show -> system -> setting -> multi-vsys is unexpected`.
59031	When admin users tried to login to the CLI without previously logging into the web interface and there was a RADIUS authentication profile configured, the firewall sent out a request to the RADIUS server with an invalid password that was different from the one submitted by the user. This resulted in valid users being unable to authenticate to the RADIUS server.
59030	Certificates generated during SSL decryption were not adhering to the ASN.1 format. This was leading to the SSL connection being dropped by some servers.
58885	The `test nat-policy-match` command now properly displays results for no-nat rules.
58736	WildFire email notifications did not contain a date header.
58733	The fields in the CSV report were displayed incorrectly after performing a CSV export on the **Monitor > HIP Match** page on the Panorama web interface.
58614	Local users discovered by WMI query were mapped as the local user of the computer, instead of Unknown as is the expected behavior.
58347	Suppressed extraneous messages (for example, disabling of an interrupt request that occurs within the underlying subsystem) from displaying on the console. These messages are now logged in the system log only.
58264	Previously, the `debug software virt-limit limit` command showed an incorrect max value: `4294967295`. The max value has been fixed to display in kilobytes.
58223	Captive portal was not presenting a complete certificate chain to the client. It presented only the end certificate and not the intermediate certificate.
58215	The output from the `show routing protocol ospf area` CLI command was rearranged to provide greater clarity in the values defined.
57975	It was not possible using Panorama to proxy a REST API call for retrieving report information from a firewall.

Issue Identifier	Issue Description
57960	When the Palo Alto Networks firewall was configured to support several virtual systems, the firewall administrator could not revert the **Destination Interface** in a NAT Policy Rule back to the option any after an interface had been selected. This was because the any field in the NAT to-interface configuration had an incorrect schema value. The incorrect schema was fixed by adding any as a default NAT to-interface value in the configuration.
57927	When authenticating through captive portal, there was a delay after the authentication redirect for Firefox and Chrome browsers. This has been corrected by closing the socket after the redirect.
57874	DNS resolution did not turn off when the **Resolve Hostname** checkbox was cleared in the **Monitor** tab, and the Palo Alto firewall continued to display the hostnames instead of the IP addresses. IP addresses are now displayed when the **Resolve Hostname** checkbox is cleared.
57768	A DHCP server did not differentiate between DHCP Clients when the DHCP Client Identifier in the DHCP request exceeded 32 bytes. The maximum size of the DHCP Client Identifier has been increased to 312 bytes.
57660	PA-2000 Series platform management ports did not link-up when connected directly using a straight or cross cable.
57608	When using multiple NetFlow hosts across multiple profiles, instances of the FlowSequence number were skipped. The expected behavior is that the value is cumulative, and should be used by the Collector to identify whether any Export Packets have been missed.
57535	Fixed an issue where the user was not able to create a QoS profile with an egress bandwidth greater than 50 Mbps on a virtual firewall (**Network > Network Profiles > QoS Profile**).
57507	The option **L3 Forwarding Enabled** in the configuration of a VLAN has been removed. In pre-6.0 releases, enabling or disabling this option did not have an effect on traffic forwarding. Enabling or disabling L3 forwarding on a VLAN should be performed by adding or removing an L3 VLAN interface to the VLAN configuration.
57448	The **IRC** checkbox in the Botnet Configuration window (**Monitor > Botnet**) was not displayed on the web interface when the language was set to Japanese and a Chrome browser was being used.
57360	CLI help for `show session all filter destination` command is showing `<ip/netmask>` instead of `<ip>`.
57258	Both HTTP and HTTPS were available when accessed directly from the management interface; however, HTTP was unavailable when accessed using a subinterface.
57159	The dataplane was passing traffic even though the management plane was rebooted and could not boot.
57154	On a PA-5000 series firewall, the QoS rate is adjusted slightly to accommodate hardware limitations. The following help message now is displayed on the configuration window on the web interface: `Bandwidth limits shown include hardware adjustment factor.`
57098	In some Layer 2 configurations, multicast traffic passing through the firewall was resulting in both forward and drop counters incrementing due to the packets being broadcast. Additionally, the multicast packet was included in both the transmit and drop stage dataplane packet capture. New global counters were added to clarify the actions being taken by the firewall when processing multicast packets in a Layer 2 configuration.

Issue Identifier	Issue Description
56905	When a PA-5000 Series firewall received more than 3000 BGP prefixes, the web interface showed an error when displaying the Local RIB for BGP: `op command for client routed timed out`. Additionally, when the `show routing protocol bgp loc-rib-detail` command was issued, the CLI returned the error: `Server error : op command for client routed timed out`.
56858	A cache corruption prevented the user from downloading files when clicking the Continue button in the File Blocking Continue page.
56802	In a single-vsys setup, a Log Forwarding Profile created on the web interface was not displayed after issuing the `show shared log-settings profile` CLI command.
56787	After an upgrade, the captive portal custom response page shows `::ffff:` before the IP address.
56703	In the web interface, global timeout values were displayed in addition to the application level timeout values that actually took effect. This has been updated to show only application level timeout values.
56367	Fixed an issue where NetFlow data could not be exported for all subinterface types. NetFlow records were not picked up by the log-receiver.
56107	Addressed dataplane restarts that occurred intermittently on the PA-3000 Series devices deployed in a high availability (HA) configuration.
56087	Log collectors were optimized in PAN-OS 6.0 for quicker failover and failback.
55833	GRE port information was not mapped correctly on the VM-Series platforms, causing predict sessions to not match and leading to dropped packets.
55774	On the web interface, setting the value for max-rows-in-csv-export did not work when it was set to more than 65535.
55696	Misspellings were displayed in the output for the `set session processing-cpu` command. The misspellings have been corrected.
55693	Added an enhancement to reduce the routed log in order to help reduce OSPF flaps.
55407	User-ID virtual memory was exceeding its limit in a multi-vsys environment when a large number of LDAP objects were returned to the firewall. With this fix, LDAP queries made by the firewall will filter on groups specified in the include-list.
55387	When using local user groups to assign users to particular gateways, the connection to the Global Protect server for the users in that local group failed.
55342	When an LDAP Server Profile was configured with multiple LDAP servers and/or multiple User-ID agents were configured to be used as LDAP proxy servers and the primary server was not connected, the firewall continually attempted to connect to the secondary LDAP server (or LDAP proxy server) but was unable to establish a connection.
55111	Fixed an issue where a FIN packet was dropped when the sequence number was out of sync after traffic triggered session reuse and was offloaded. With this fix, the sequence-number check for offloaded reused sessions is skipped (because the data plane processor cannot track sequence numbers after traffic is offloaded).
54958	Upon opening a PCAP on the firewall, escape sequences were displayed instead of the special characters in data part. A fix is provided to display the characters correctly.

Issue Identifier	Issue Description
54949	A commit failed when DHCPv6 relay was configured on an interface that did not have an IPv4 address.
54755	An issue was addressed where creating a static route with the next hop set to None and cloning it or going back into it was changing the next hop settings to <IP Address> from None.
54676	In the web interface, on the **Device > User Identification > Group Mapping Settings > Group Mapping > Group Include List** tab, the list of Available Groups to add to the Included Group list displayed approximately the first 200 groups, with the option to select **more** to view more group entries. However, clicking **more** failed to display more group entries, even when several more groups are defined and should be available.
54547	Fixed an issue where high availability (HA) peer HA2 IP information was not getting updated after issuing the `show high-availability all` CLI command.
54486	Added support for both single quote and double quote values when entering options using the Command Line Interface (CLI).
54283	An auto commit failed during a threat database update, displaying the error `Threat database handler failed`.
54265	The system log message `Antivirus job failed` has been updated and the following will be reported in the system log instead: `Antivirus update job failed`.
54113	A Forwarding Information Base (FIB) table entry discrepancy caused SSH packets to be sent back. This only occurred on PA-2000 Series firewalls.
53888	On PA-5000 Series devices, the DIPP limit was causing the following system error when trying to add more NAT policies to the firewall: `Error: Number of dynamic-ip-and-port rules (251) exceeds vsys capacity (250) Error: Failed to parse nat policy The maximum number of DIPP has now been increased.`
53632	Fixed a BGP aggregate policy issue where the aggregate route was no longer advertised when a more specific prefix within the aggregate range was learned.
53615	When enabling IPv6 on an interface, link local IPv6 routes were counted towards the rtm_total/connected/ipv6; however, the Link Local IPv6 routes were not installed to the Forward Information Base (FIB) on the dataplane.
53554	Disks in a Panorama VM OVF were misaligned with NetApp and caused performance degradation with some storage devices.
53514	A high availability (HA) active/active configuration for IPv6 using Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) did not behave consistently when stateless address autoconfiguration (SLAAC) was also configured.
53148	Output of `debug dataplane packet-diag show setting` command truncates the interface name to 15 characters.
53059	Role-based admin users without privileges to access logs or the **Monitor** tab were able to view logs using the **Dashboard** widgets.
52847	Link monitoring and Path monitoring were on hold when a commit started and until one minute after the commit was done. Changes are introduced to remove the hold on the Link and Path monitoring during Phase -1 of commits.
52777	Link and Path monitoring were not always working properly during the commit process.

Issue Identifier	Issue Description
52738	Reset was sent to Captive Portal clients when trying to load multiple pages before logging in to the portal.
52629	PAN-DB reverted back to BrightCloud due lack of management connection for first reboot.
52567	The loading icon was not shown when using the list of users to add a source user to a security policy on the web interface.
52214	Some traffic was getting dropped if the number of routes in the routing table was high.
52184	Changing the Jumbo Frame settings on the device without restarting the entire device caused the dataplane to experience an unexpected restart. This has since been fixed so that when you change Jumbo Frame settings, an entire device reboot is no longer required and a dataplane restart will work.
52128	Fixed an issue where a management profile was configured on an interface and the clients were not getting IP addresses from the DHCP server when the device was configured as a DHCP relay agent.
52050	After manually upgrading PAN-OS, no **Reboot** button was visible, as it was in previous releases. A message was displayed instead that the user must reboot the device by closing the current window and then rebooting.
51955	The CLI displayed two counters listed under `IPv6 filter`, even though they also applied to IPv4. A change was made to list them under `IPv(4/6) filter`.
51880	Dynamic role-based device administrators did not have the ability to save, export, load, and revert a configuration on the firewall or Panorama. This fix provides these capabilities to the administrators.
51824	Device Groups added to multiple virtual systems were not always shown as managed devices on the web interface (**Panorama > Device Groups > Device Group**).
51648	In a high availability (HA) active/passive configuration, if NAT exists for outbound FTP connections and the interface IP address is used for the NAT, the ftp-data session would not synchronize to the passive device.
51597	When the XML API was used to push IP address, port range and username information to a firewall deployed in high availability (HA) configuration, the details were not synchronized with the HA peer.
51091	Two-factor authentication (where both a client certificate profile and an authentication profile are configured) was not functioning as expected. The client was not required to provide the login credentials associated with the authentication profile after successfully authenticating with the client certificate.
51089	Fixed an issue where repeat count in threat logs was resulting in incorrect values.
51062	Inter-vsys sessions that traverse the firewall and terminate on a firewall interface would fail. This has been fixed.
51042	Certificates that were generated prior to master key changes could continue to be used.
51000	On a redundant Power Supply system on a PA-5000 Series device, there was no system log visible when removing or adding redundant Power Supply. Logging for these events has been added.
50963	Panorama software deployment failed to deploy when the **OK** button was clicked.

Issue Identifier	Issue Description
50936	Crypto cores were created when a SIGTERM signal was received while the management plane was starting.
50817	Fixed an issue for firewalls running PAN-OS 4.1.6 and later releases where GlobalProtect users were unable to connect to the GlobalProtect gateway when the external-facing interface on the gateway was configured with dynamic PPPoE and a loopback interface was configured for the destination interface to the GlobalProtect portal. With this fix, you can configure a loopback interface for GlobalProtect even when the external-facing interface for the gateway is dynamic.
50606	Captive Portal authentication failed when the username contained the character &. This issue has been addressed so that & is a valid character and Captive Portal authentication is successful when a username contains the character &.
50478	The certificate signing request (CSR) generated by the firewall had a Challenge Attribute set by default. If configured, the signing entity could use this attribute or ignore it. Since this attribute was not being ignored by some signing entities, the behavior has been updated so that the Challenge Attribute is not set by default.
50310	A destination based service route for DNS prevented an FQDN query from refreshing.
50091	A possible memory leak caused management plane services to not perform optimally during peak traffic periods.
50079	Added logging enhancements in order to help identify root cause.
50048	The `show session all filter from <zone> to <zone>` CLI command displayed no active sessions when there were active sessions that should have been displayed in the output.
49851	In PAN-OS 6.0, DoS enforcement is now performed in CPU prior to session installation.
49828	In custom reports, source and destination country are now available in the Query Builder as grouping options to organize the report.
49727	Navigating to the **Network > Interface > Ethernet** tab took 12-15 seconds for the screen to populate the interface data.
49294	The **ACC** (Application Command Center) tab on the Panorama web interface failed to display complete sections and appeared to be stalled, showing the error message: `3 requests sent 1 response received`.
49038	Time zones were not automatically converted for Dynamic Update package release times.
49015	Fixed a dataplane restart issue that occurred when Jumbo Frames were enabled and the packets received buffer was high.
48896	In rare cases, abrupt restarting (for example, a power outage) lead to internal system file corruption. This was related to checking OS image integrity and cannot upgrade. Preventative measures were put in place to prevent issues before and after the internal file updating.
48729	In Panorama, disabling the **Share Unused Address and Service Objects with Devices** feature returned an error stating that the shared address is not a valid reference. This occurred when a non-shared address group—that was assigned to a specific device group—contained a shared address or an address group was pushed. This issue has been fixed so that such a configuration is supported.

Issue Identifier	Issue Description
48709	Fixed an issue where setting a packet capture filter in the web interface did not work until the filter was reset by removing the automatically added 0.0.0.0.
48703	This fixes a NAT pool leak issue when a SYN packet on TCP/443 was sent to an address on an interface on which GlobalProtect was configured but which was not its primary address. A NAT port was allocated, the connection failed, and the session was freed, but the allocated NAT port is not cleared.
48584	On Panorama, there were long delays committing a policy due to the option **Share Unused Address and Service Objects with Devices** being cleared in large configurations. The delay was introduced as the system performs a calculation of the unused objects on commit. Commit times have been improved for large configurations.
48093	Configured address objects were not displayed as resolved on the Panorama web interface. On both the **ACC** tab and the **Monitor > Logs > Traffic** tab, host names defined in the address objects were not displayed, and the IP address was shown in the Host Name columns.
47616	Devices which were no longer managed devices (had been managed devices previously but were not anymore) were displayed on the **Panorama > Device Deployment > Licenses** page on the Panorama web interface.
47461	Fixed an issue where SIP sessions were going into offload state after a content installation causing SIP connectivity issues.
47071	In PAN-OS 6.0.0, you can now rename and push a shared object from Panorama to a managed firewall if you used that shared object in a local policy.
47007	An enhanced mechanism to hold control session packets being sent out before predict session is now installed on the master dataplane.
46535	When using an Internet Explorer browser and a Block / Continue page appears when attempting to download a file, clicking the Continue option did not download the file.
46308	The full User-ID Mapping table is now synchronized between peers in a high availability (HA) cluster.
46134	On the Panorama web interface, DHCP server settings displayed for entries on the **Network > DHCP** page were not displayed on the DHCP Server window that is displayed when clicking on one of the specific DHCP server entries.
45529	In some User-ID implementations, server session reads picked up capitalized special characters such as Ü. Normally all capitals are set to lower case, but this operation was not supported for special characters, causing a mismatch between group mapping and ip mapping.
44925	When a Virtual Router interface was deleted, added, or updated with a new IP/mask, all local Virtual Router interfaces on the management plane were uninstalled and then reinstalled. With this fix, the management plan will assess if all Virtual Router interfaces change before automatically uninstalling and reinstalling them all; the management plane will not continue to uninstall and reinstall all Virtual Router interfaces unless they have all been changed.
43280	Prior to PAN-OS 6.0.0, NetFlow data could not be exported on a per subinterface basis. Starting in PAN-OS 6.0.0, NetFlow data can be exported on a per subinterface basis.

Issue Identifier	Issue Description
41472	When a DNS Proxy object was configured with static entries, hostnames assigned to the DNS Proxy were resolved as expected to the IP addresses listed on the Static Entries tab (**Network > DNS Proxy**). However, when setting the DNS Proxy Object as the DNS Service on the **Device > Setup > Services** dialog, all DNS queries from the management interface ignored the defined static entries.
40648	Validation logic has been added to PAN-OS software image files to prevent upgrade failures due to file corruption.
39368	Enhancements have been made to the web interface so that high availability (HA) link status is displayed with green or red indicators on the **High Availability** widget on the **Dashboard** tab. A green indicator signifies that the link is up on the HA port and heartbeats (keep-alive messages) are being sent and received. A red indicator signifies that the link on the HA port is down or that heartbeats (keep-alive messages) are not being received at all. (For HA3 interfaces, the green and red indicators signify only whether the link is up or down.)

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 6.0
  - Panorama 6.0
  - WildFire 6.0

Requesting Support

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

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

Contact Information

Corporate Headquarters:

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

www.paloaltonetworks.com/company/contact-us

Palo Alto Networks, Inc.

www.paloaltonetworks.com

Revision Date: November 16, 2016