PAN-OS® 7.0 Release Notes

Release 7.0.16

Revision Date: June 6, 2017

Review important information about Palo Alto Networks PAN-OS 7.0 software, including new features introduced, workarounds for open issues, and issues that are addressed in the PAN-OS 7.0 release. For installation, upgrade, and downgrade instructions, refer to the PAN-OS 7.0 New Features Guide. For the latest version of these release notes, refer to the Palo Alto Networks technical documentation portal.

⚠ The Panorama certificate used to authenticate Panorama-to-firewall communication expires on June 16, 2017. Review the most current information about how to make sure you can continue using Panorama to manage firewalls and to aggregate firewall logs on Log Collectors after June 16, 2017: https://live.paloaltonetworks.com/t5/General-Topics/Panorama-Certificate-Expiration-on-June-16-2017/m-p/150948/thread-id/50050. (Physical and virtual firewalls, WF-500 appliances, and M-500 appliances running in PAN-DB mode do not require any action.)

PAN-OS 7.0 Release Information

The Panorama certificate used to authenticate Panorama-to-firewall communication expires on June 16, 2017. Review the most current information about how to make sure you can continue using Panorama to manage firewalls and to aggregate firewall logs on Log Collectors after June 16, 2017: https://live.paloaltonetworks.com/t5/General-Topics/Panorama-Certificate-Expiration-on-June-16-2017/m-p/150948/thread-id/50050. (Physical and virtual firewalls, WF-500 appliances, and M-500 appliances running in PAN-DB mode do not require any action.)

Features Introduced in PAN-OS 7.0

The following topics describe the new features introduced in PAN-OS® 7.0 releases, which require content release version 497 or a later version. For upgrade and downgrade considerations and for specific information about the upgrade path for a firewall, refer to the Upgrade section of the PAN-OS 7.0 New Features Guide. The new features guide also provides additional information about how to use the new features in this release.

- ▲ Management Features
- ▲ Panorama Features
- ▲ WildFire Features
- ▲ Content Inspection Features
- ▲ Authentication Features
- ▲ Decryption Features
- ▲ User-ID Features
- ▲ Virtualization Features
- ▲ Networking Features
- ▲ Policy Features
- ▲ VPN Features
- ▲ GlobalProtect Features
- ▲ Licensing Features

Management Features

New Management Feature	Description
All New Application Command Center (ACC)	The ACC is redesigned to provide improved visibility into network traffic and actionable information on threats. The new layout includes a tabbed view of network activity, threat activity, and blocked activity and each tab includes pertinent widgets for better visualization of traffic patterns on your network. For a personalized view of your network, you can also add a custom tab and include widgets that allow you to drill down into the information that is most important to you.
Automated Correlation Engine	The new automated correlation engine is an analytics tool that detects security events on your network. It collects isolated events across multiple log types on the firewall, queries the data for specific patterns, and correlates network events to identify actionable information such as host-based activities that indicate a compromised host. The automated correlation engine includes *correlation objects* that are defined by the Palo Alto Networks Malware Research team. These objects identify suspicious traffic patterns or a sequence of events that indicate a malicious outcome; some correlation objects can identify dynamic patterns that have been observed from malware samples in WildFire™. Correlation objects trigger *correlation events* when they match on traffic patterns and network artifacts that indicate a compromised host on your network. Thus, correlated events provide actionable intelligence that you can use to remediate incidents, mitigate risks, and secure your network. You can view the correlated event logs in the Monitor tab or see a graphical display in the Compromised Hosts widget on the Threat Activity tab of the ACC. The automated correlation engine is supported on PA-3000 Series, PA-5000 Series, PA-7000 Series platforms, and on Panorama™. New correlation objects will be delivered with the weekly content updates. To obtain new correlation objects, the firewall must have a Threat Prevention license; Panorama requires a support license for getting the correlation objects with the weekly content updates.
Global Find	To make the management of your Palo Alto Networks devices more efficient, a new global find feature is introduced to enable you to search the entire configuration of a PAN-OS or Panorama web interface for a particular string, such as an IP address, object name, policy name, threat ID, or application name. The search results are grouped by category and provide links to the configuration location in the web interface, so that you can quickly and easily find all of the places where the string is referenced. For example, if you temporarily denied an application that is defined in multiple security policy rules and you now want to allow that application, you can search on the application name and quickly locate all referenced polices to change the action back to allow.
Tag Browser	The tag browser introduces a way to view all the tags used within a rulebase. In rulebases with a large number of rules, the tag browser simplifies the display by presenting the tags, the color code, and the rule numbers in which the tags are used; it also allows you to group rules using the first tag applied to the rule. You can, for example, filter rules by the first tag applied and view the rules grouped by a high-level function such as internet access or data center access. In this grouped-rule view, if you identify gaps in coverage, the tag browser allows you to move rules or add new rules within the rulebase.
Configuration Validation Improvements	The option to validate a PAN-OS or Panorama candidate configuration before you commit (to determine whether your recent changes will commit successfully) is enhanced to do syntactic and semantic validation of the configuration. It then displays the same errors and warnings as would display for a full commit or virtual system commit, such as rule shadowing or application dependency warnings, or errors indicating an invalid route destination or a missing account/password to query a server.

New Management Feature	Description
Move and Clone Policies, Objects, and Templates	You can now move or clone policies and objects to a different device group or virtual system. This saves you the effort of deleting, recreating, or renaming these items when only a move or copy is needed. You can also clone templates and Template Stacks.
Extended SNMP Support	Extended SNMP support includes: • Global counters for Denial of Service (DoS), IP fragmentation, TCP state, and dropped packets, by which to monitor the health and security of your devices and network. Previously, you had to use the CLI or XML API to monitor global counters. • SNMP Interface MIB for Logical Interfaces—The PAN-OS implementation of the interfaces and IfMIB has been extended to support all logical interfaces on the firewall, including tunnels, aggregate groups, L2 subinterfaces, L3 subinterfaces, loopback interfaces, and VLAN interfaces. This is in addition to the SNMP Interface MIB support on physical interfaces. In addition, the VPN tunnel status can now be monitored. • LLDP-V2-MIB—Information transmitted and received from neighbors using Link Layer Discovery Protocol (LLDP) is stored for SNMP access. All MIB objects under the standard LLDP MIB definitions are supported. Neighbor entries are aged out when their TTL value contained in the received LLDP message reaches zero.
SaaS Application Usage Report	A new predefined report is introduced to provide visibility into Software as a Service (SaaS) application usage, enabling you to assess and subsequently mitigate the risks to your enterprise's data when taking advantage of SaaS applications. The report will also help to assess risks to the security of your enterprise network, such as the delivery of malware through SaaS applications adopted by your users.
Policy Impact Review for New Content Releases	Before installing a new content release, you can now review the policy impact for new App-IDs™ and stage any necessary policy updates. This enables you to assess the treatment an application receives both before and after the new content is installed and then prepare policy updates to take effect at the same time that the content update is installed. This feature specifically includes the capability to modify existing security policies using the new App-IDs contained in a downloaded content release (prior to installing the new content). You can then simultaneously update your security policy rules and install new content, allowing for a seamless shift in policy enforcement. You can also choose to disable new App-IDs when installing a new content release version; this enables protection against the latest threats, while giving you the flexibility to enable the new App-IDs after you've had the chance to prepare any policy changes.
Security Profile and Address Objects Per Address Group Capacity Increase	The security profile capacities and number of address objects per address group have been increased as follows: • **Security Profile**—Capacity increased on all platforms by approximately 50% for the following security profiles: Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, WildFire Analysis, Data Filtering, and Decryption. For example, the PA-7050 firewall supported 500 security profiles in PAN-OS 6.1, and now supports 750 profiles in PAN-OS 7.0. • **Address objects per address group**—Increased from 500 to 2500 for all platforms. For details on platform capacities, refer to https://www.paloaltonetworks.com/products/product-selection.html.
Virtual System/Device Name in Reports and Logs	You can now view or search logs or create a report based on virtual system names and device names, which are more user-friendly attributes to use than virtual system IDs and device serial numbers. Now you do not need to manually map a virtual system name to its ID or map a device name to its serial number, to view or search logs or create reports. Virtual System Name and Device Name are added as available attributes to PAN-OS and Panorama reports and logs.

New Management Feature	Description
Time-Based Log and Report Deletion	You can now configure automatic deletion of logs and reports based on time instead of just on space quotas. This is useful in deployments where periodically deleting monitored data is desired or necessary. For example, deleting user data after a certain period might be mandatory in your organization for legal reasons.
Software Upload Improvements	Devices now display details about uploaded software updates that enable you to check, before installing an update, that it is the intended one. Installing uploaded software now involves fewer steps, which makes deployment easier when a device does not have external network access.

Panorama Features

New Panorama Feature	Description
Device Group Hierarchy	You can now create nested device groups in a tree hierarchy with lower-level groups inheriting the settings of higher-level groups. This enables you to organize devices based on function and location without redundant configuration. For example, you could configure Shared settings that are global to all firewalls, configure device groups with function-specific settings at the first level, and configure device groups with location-specific settings at subsequent levels. Without a hierarchy, you would have to configure both function- and location-specific settings for every device group in a single level under Shared. Combined with the Role-Based Access Control Enhancements in this release, a hierarchy also enables you to control administrator access to data according to areas/levels of responsibility.
Template Stacks	You can now define a template stack, which is a combination of templates. By assigning firewalls to a stack, you can push all the necessary settings to them without the redundancy of adding every setting to every template. For example, you could assign the firewalls in a California data center to a stack that has one template with global settings, one template with California-specific settings, and one template with data center-specific settings. To manage firewalls in a California branch office, you could then re-use the global and California-specific templates by adding them to another stack that includes a template with branch-specific settings.
Role-Based Access Control Enhancements	You can now associate each access domain with an administrator role to enforce the separation of information among the functional or regional areas of your organization. You can assign multiple access domain/role pairs to an administrator (local or external), who can then filter the Panorama web interface to display only information that is relevant to a particular domain. For custom roles, you can also define feature-specific access to firewalls (through context switching) separately from Panorama access, and provide additional access to logs and reports, so that administrators can have a broader range of responsibilities.
Firewall Configuration Import into Panorama	You can now import firewall configurations into Panorama instead of recreating them. Panorama provides the option to import objects from Shared on the firewall into Shared in Panorama, and import other objects, policies, and settings into new device groups and templates. After the import, you can Move and Clone Policies, Objects, and Templates to different device groups.

New Panorama Feature	Description
Panorama Support for Larger Configuration Files	Panorama now supports much larger configuration files, which enable you to add more information and greater complexity to individual device groups, templates, and other configurations without affecting system performance or stability. Panorama also supports a higher number of concurrent, active administrators.
Log Redundancy Within a Collector Group	You can now enable log duplication for a Collector Group so that each log will have two copies and each copy will reside on a different Log Collector. This redundancy ensures that, if any one Log Collector becomes unavailable, no logs are lost: you can still display all the logs forwarded to the Collector Group and run reports for all the log data.
Firewall HA State in Panorama	The Panorama web interface now displays the high availability state of firewalls (for example, active or passive) in places where knowing that state is useful. For example, the **Context** drop-down now displays HA state so that you can switch context to the active-primary firewall when you need to change the firewall configuration.
Scheduled Updates for Antivirus, WildFire, and URL Filtering on Log Collectors	In PAN-OS 7.0.3 and later releases, you can schedule Antivirus, WildFire, and URL Filtering (BrightCloud only) updates for Log Collectors using the Panorama web interface (**Panorama > Device Deployment** > **Dynamic Updates** > **Schedules**) or the CLI. For reporting consistency, configure scheduled content updates for all log collectors to ensure they stay in sync.

WildFire Features

New WildFire Features	Description
Grayware Verdict	The WildFire grayware verdict is introduced to clearly identify executables that behave similarly to malware but are not malicious in nature or intent. A grayware verdict might be assigned to executables that do not pose a direct security threat but display otherwise obtrusive behavior (for example, installing unwanted software, changing various system settings, or reducing system performance). Examples of grayware software typically include adware, spyware, and Browser Helper Objects (BHOs). The grayware verdict allows the security responder to quickly distinguish malicious files on the network from grayware and to prioritize accordingly. While antivirus signatures are not generated for grayware, WildFire logs can continue to alert the security responder to endpoints downloading grayware so the responder can assess whether such events are concerning.

New WildFire Features	Description
WildFire Hybrid Cloud	Enable a WildFire hybrid cloud deployment so that a single firewall can forward unknown samples (files or email links) to either a WF-500 appliance or the WildFire public cloud, depending on the sample. This feature allows the flexibility to analyze private documents inside the network, while files sourced from the internet can be analyzed by the WildFire public cloud. For example, Payment Card Industry (PCI) and Protected Health Information (PHI) data can be exclusively forwarded to the WF-500 appliance for private cloud analysis and less sensitive files, such as Portable Executables (PEs), can be forwarded to the WildFire public cloud. When possible, offloading files to the WildFire public cloud allows you to benefit from a prompt verdict for files that have been previously processed by the public cloud and also frees up WF-500 appliance capacity to process sensitive content. Additionally, in a WildFire hybrid cloud deployment, you can use the WildFire public cloud to analyze file types that are not currently supported for WF-500 appliance analysis, such as Android Application Package (APK) files. This feature also introduces the WildFire Analysis profile, to be used in place of the file blocking profile to forward samples for WildFire analysis. Existing File Blocking profile rules with the action set to **forward** or **continue and forward** are migrated to the new WildFire Analysis profile. For each WildFire analysis profile rule, define traffic to forward to either the WildFire private cloud or the WildFire public cloud based on file type, application, or file transfer direction (upload or download).
WildFire Appliance Support for Java Antivirus Signatures	The WildFire appliance can now locally generate antivirus signatures for malicious Java files (.jar and .class), so that malicious Java files detected by the WildFire appliance no longer have to be forwarded to the WildFire Cloud for signature generation.
WildFire Appliance Support for Email Link Analysis	The firewall can now extract HTTP/HTTPS links contained in SMTP and POP3 email messages and forward the links to the WildFire appliance for analysis (this feature was supported only for the WildFire public cloud in PAN-OS 6.1). Enable this functionality by configuring the firewall to forward the email-link file type (**Objects** > **Security Profiles** > **WildFire Analysis**). Note that the firewall only extracts links and associated session information (sender, recipient, and subject) from the email messages that traverse the firewall; it does not receive, store, forward, or view the email message. After receiving an email link from a firewall, the WildFire appliance visits the link to determine if the corresponding web page hosts any exploits. If it detects malicious behavior on the page, it returns a malicious verdict and: • Generates a detailed analysis report and logs it to the WildFire Submissions log on the firewall that forwarded the links. • Categorizes the URL as malware and generates and distributes a signature to connected firewalls to allow them to identify and block the malware. If the link corresponds to a file download, the WildFire appliance does not analyze the file. However, the firewall will forward the corresponding file to the WildFire appliance for analysis if the end user clicks the link to download it as long as the corresponding file type is enabled for forwarding. The WildFire appliance does not send a log to the firewall if it determines a link to be benign or grayware—even if you enabled logging of benign or grayware files—because of the large number of logs this would generate.

Content Inspection Features

New Content Inspection Features	Description
Configurable Drop Actions in Security Profiles	The Vulnerability Protection, Anti-Spyware, and Antivirus profiles include new actions to drop or reset connections. In addition to the allow/alert/block actions within the security profile, you can now granularly define how to drop or reset connections when the firewall detects a threat. For example, to secure the Microsoft web servers on your network, you can create a rule in the Vulnerability Protection profile with an action to either drop the traffic and send a reset only to the server or drop the traffic and block the offending client IP address from creating new connections for a specified time interval.
Increased Inspection Depth for Multi-Level Compression and Encoding	The firewall now identifies and inspects files that have been encoded or compressed up to four times, where previously the firewall supported only two levels of decoding. Multiple levels of compression and encoding are frequently introduced to files based on the file format and the application used for file transfer. For example, a Microsoft Office Open XML file (.docx) that is compressed (.zip) and is sent as an email attachment has three levels of encoding: the OOXML format is one level of encoding, the compression of the file to the ZIP format is the second level of encoding, and the third level of encoding is added when the email attachment is embedded using Base64. In this case, the firewall now decodes the file, correctly identifies it as a Microsoft Word document, and performs policy-enforcement including file blocking, threat inspection, and WildFire analysis.
Blocking of Encoded Content	A new file type classification, Multi-Level-Encoding, can now be used to log or block content that has been compressed or otherwise encoded to a high degree. As the firewall can now decode and inspect up to four levels of encoding (see Increased Inspection Depth for Multi-Level Compression and Encoding), the new classification can be used to block files that have been encoded five times or more. Multiple levels of encoding can be used as an evasion technique to circumvent security devices; using the Multi-Level-Encoding file type to perform file-blocking ensures that unidentified files that have not been processed for threats are not passed through the firewall.
Negate Operator for Custom Threat Signatures	A new **Negate** operator is now available when creating custom vulnerability or spyware signatures. The **Negate** operator can be used to ensure that the vulnerability or spyware signature is not triggered under certain conditions. For example, create a custom signature to trigger when a Uniform Resource Identifier (URI) pattern is matched to traffic but only when the HTTP referer field is not equal to a certain value. A custom signature must include at least one positive condition for a negated condition to be specified.
PAN-DB Private Cloud	If the security and compliance requirements in your enterprise prohibit the Palo Alto Networks next generation firewalls from directly accessing the internet for performing URL look ups, you can deploy a PAN-DB private cloud. To protect users from malware and undesirable web content, the firewalls can query the PAN-DB private cloud deployed within your network instead of accessing the PAN-DB public cloud. The PAN-DB private cloud solution ensures information privacy and does not send any data or analytics to the public cloud.

Authentication Features

New Authentication Features	Description
Authentication and Authorization Enhancements	The workflow to configure authentication servers and profiles is now more intuitive and consistent. You can also enable GlobalProtect™ clients to send RADIUS vendor-specific attributes to RADIUS servers so that RADIUS administrators can make policy decisions based on those attributes. For example, RADIUS administrators might use the client operating system attribute to define a policy that mandates regular password authentication for Microsoft Windows users and one-time password (OTP) authentication for Google Android users.
SSL/TLS Service Profiles	You can now assign SSL/TLS service profiles to device services that use SSL/TLS, including Captive Portal, management traffic access using the web interface or XML API, the URL Admin Override feature, the User-ID™ Syslog listening service, and you can assign profiles to GlobalProtect portals and gateways. SSL/TLS service profiles specify a certificate and the allowed protocol version or range of versions (now including TLSv1.2). By defining the protocol versions, the profiles enable you to restrict the cipher suites that are available to secure communication with enpoints that are requesting the services. This improves network security by allowing you to configure endpoints to avoid SSL/TLS versions that have known weaknesses.
TACACS+ Authentication	Devices now support the Terminal Access Controller Access-Control System Plus (TACACS+) protocol for authenticating administrative users. TACACS+ provides greater security than RADIUS insofar as it encrypts usernames and passwords (instead of just passwords) and is also more reliable (uses TCP instead of UDP).
Kerberos Single Sign-on	Devices now support Kerberos V5 single sign-on (SSO) for administrator authentication and Captive Portal authentication. Single sign-on minimizes the number of logins requiring user input while ensuring security for web services.
Suite B Cryptography Support	You can now use Suite B ciphers to authenticate administrators, to secure site-to-site VPN, and to secure GlobalProtect remote access and large scale VPN (LSVPN). To secure the VPN tunnels between GlobalProtect LSVPN gateways and endpoint devices, the latter must run GlobalProtect client agent 2.2 or a later release. The new GlobalProtect IPSec Crypto profile supports Suite B encryption algorithms (and other algorithms) for LSVPN. You can use elliptic curve (ECDSA) certificates for administrator and GlobalProtect authentication. Suite B support enables you to meet U.S. federal network security standards.
Authentication Server Connectivity Testing	You can now test an authentication profile to determine if your firewall or Panorama management server can communicate with a backend authentication server and if the authentication request was successful. You can perform authentication tests on the candidate configuration, so that you know the configuration is correct before committing. Authentication server connectivity testing is supported for local database, RADIUS, TACACS+, LDAP, and Kerberos authentication.

Decryption Features

New Decryption Features	Description
SSL Decryption Enhancements	When using SSL decryption to inspect and enforce security rules for connections between clients and destination servers, enable the following new options as increased security measures: • Enforce the use of strong cipher suites. This includes support to specifically enforce the use of AES128-GCM and AES256-GCM ciphers. • Enforce the use of minimum and maximum protocol versions. • Enforce certificate validation on a per-policy basis (where previously, certificate validation was performed at the device level). • Define traffic that you want to be decrypted based on TCP port numbers. This enables you to apply different decryption policies to a single server's traffic; traffic being transmitted using different protocols can receive different treatment. • Enforce valid certificates and trusted issues for traffic that is not decrypted, with the options to terminate an SSL session if the server certificate is expired or if the server certificate issue is untrusted.

User-ID Features

New User-ID Feature	Description
User Attribution Based on X-Forwarded-For Headers	You can now configure User-ID to read user IP addresses from the X-Forwarded-For (XFF) header in client requests for web services when the firewall is deployed between the internet and a proxy server that would otherwise hide the user IP addresses. User-ID matches the IP addresses with usernames that your policies reference so that those policies can control and log access for the associated users and groups.
Custom Groups Based on LDAP Filters	You can now define custom groups based on LDAP filters so that you can base firewall policies on user attributes that do not match existing user groups in an LDAP-based service such as Active Directory (AD). Defining custom groups can be quicker than creating new groups or changing existing ones on the LDAP server and does not require an LDAP administrator to intervene.

Virtualization Features

New Virtualization Feature	Description
Support for High Availability on the VM-Series Firewall	The VM-Series firewall on ESXi, Xen (on SDX), and KVM now supports both Active/Passive HA and Active/Active HA with session synchronization. The VM-Series in Amazon Web Services (AWS) supports Active/Passive HA only. In an HA configuration, you must deploy both peers on the same type of hypervisor, have identical hardware resources assigned to them, and have the same set of licenses and subscriptions.

New Virtualization Feature	Description
Support for Jumbo Frames	The VM-Series firewall can now support jumbo frames, which are Ethernet packets larger than 1,500 bytes. Like with hardware-based firewalls, when you enable jumbo frames on a VM-Series firewall, the default Maximum Transmission Unit (MTU) size for all Layer 3 interfaces is set to 9,192 bytes; the MTU can range between 512 and 9,216 bytes. You can override the global MTU and configure an explicit value between 512 and 9,216 bytes on a per-interface basis.
Support for Hypervisor Assigned MAC Address	The VM-Series firewall supports the ability to detect the MAC address assigned to the physical interface by the host/hypervisor and use that MAC address on the interfaces assigned to the VM-Series firewall. In Layer 3 deployments, this capability allows a vSwitch to forward traffic to the correct interface on the firewall without requiring that promiscuous mode be enabled on the vSwitch. Hypervisor-assigned MAC addresses are also supported on PCI passthrough and SR-IOV capable network adapters.

For licensing features on the VM-Series firewall, see Licensing Features.

Networking Features

New Networking Feature	Description
ECMP	The firewall now supports Equal Cost Multipath (ECMP). Enable ECMP for the forwarding table to have up to four equal-cost paths to a single destination, which allows you to load balance traffic, use more of the available bandwidth, and have traffic dynamically shift to another ECMP member if one path fails. You can choose one of several load-balancing algorithms to determine which equal-cost path a virtual router uses for a new session to the destination.
DHCP Options	A firewall configured as a DHCP server can now send a full range of DHCP options to clients, including vendor-specific and customized options that support a wide variety of office equipment, such as IP phones and wireless infrastructure devices. Each option code supports multiple values, which can be IP addresses, ASCII text, or hexadecimal values. With the enhanced DHCP option support enabled on the firewall, branch office administrators do not need to purchase and manage their own DHCP servers to provide vendor-specific and customized options to DHCP clients.
Granular Actions for Blocking Traffic in Security Policy	When you configure the firewall to block traffic, the firewall either resets the connection or silently drops packets. When the firewall silently drops packets, it causes some applications to break and appear unresponsive to the user. New actions to gracefully block traffic provide a better user experience. The new actions available are: • Drop traffic silently and, optionally, send an ICMP Unreachable response to the user. • Block traffic and, automatically, use the deny action predefined for the application. You can view the predefined deny action for an application in Applipedia. • Reset the connection with a TCP reset on the client-side connection, on the server-side connection, or both sides of the connection. These new actions will be logged in the Traffic logs and are available for log queries.

New Networking Feature	Description
Session-Based DSCP Classification	Differentiated Services Code Point (DSCP) classification is used to indicate the level of service requested for traffic, such as high priority or best effort delivery. Set up session-based DSCP classification to enable the firewall to honor the service class requested for traffic and to mark a session to receive priority treatment. Session-based DSCP extends the power of Quality of Service (QoS), which polices traffic as it passes through the firewall, by allowing all network devices between the firewall and the client to also police traffic based on the DSCP value for the traffic. For example, inbound return traffic from an external server can now be treated with the same priority that the firewall initially enforced for the outbound flow. Network devices intermediate to the firewall and end user will also then enforce the same priority for the return traffic.
QoS on Aggregate Ethernet (AE) Interfaces	You can now enable QoS on AE interfaces configured on PA-7000 Series, PA-5000 Series, PA-3000 Series, PA-2000 Series, and PA-500 platforms. An AE interface is two or more interfaces linked together for combined bandwidth and link redundancy. When using AE interfaces to scale your network, enable QoS on an AE interface to prioritize, allocate, and guarantee the increased bandwidth supported on the AE interface. Support for QoS on AE interfaces on PA-7050 firewalls began in PAN-OS 6.0.
Improved Performance for a Single VPN Tunnel	In deployments where a single VPN tunnel is set up between a Palo Alto Networks firewall and another IPSec VPN device and where that tunnel supports multiple sessions, the firewall can now use multiple CPU cores (simultaneously) to decrypt traffic. When the volume of VPN traffic is high, this enhancement minimizes latency and improves performance.
Per-Virtual System Service Routes	The source interface and source IP address of service routes can now be configured for individual virtual systems, in addition to the global configuration of service routes. Per-virtual system service routes provide the flexibility to customize service routes for numerous tenants or departments on a single firewall. Any virtual system that does not have a service route configured to access a particular external service inherits the source interface and source IP address that are set globally for that service. The PA-7000 Series firewalls use Log Processing Card (LPC) subinterfaces to separate the logging services for each virtual system. Prior to PAN-OS 7.0, each service route to a service was configured globally and applied to the entire firewall.
LLDP	You can now configure Link Layer Discovery Protocol (LLDP) to enable the firewall to automatically discover neighboring devices and their capabilities at the link layer. LLDP allows the firewall to send and receive Ethernet frames containing LLDP data units to and from neighbors. The receiving device stores the information in a MIB, which can be accessed by SNMP. LLDP enables network devices to learn the capabilities of the connected devices and can be used to map network topology. This makes troubleshooting easier, especially for virtual wire deployments where the firewall would typically go undetected by a ping or traceroute.
NPTv6	You can now enable IPv6-to-IPv6 Network Prefix Translation (NPTv6) on the firewall to perform a stateless, static translation of one IPv6 prefix to another IPv6 prefix (port numbers are not changed). One benefit of NPTv6 is the prevention of asymmetrical routing problems that result from provider-independent addresses being advertised from multiple data centers. NPTv6 allows more specific routes to be advertised so that return traffic arrives at the same firewall that transmitted the traffic. Another benefit is the independence of private and public addresses; you can change one without affecting the other. A third benefit of NPTv6 is the ability to translate unique local addresses (ULAs) to globally routable addresses.

New Networking Feature	Description
TCP Split Handshake Drop	Palo Alto Networks firewalls by default correctly secure TCP sessions, whether they use a well-known 3-way handshake or a variation, such as a 4-way or 5-way split handshake or a simultaneous open. The firewall now offers an additional option to simply drop a TCP session that tries to use such a variation because it is possibly malicious.
Increased Address Resolution per FQDN	In pre-PAN-OS 7.0 releases, you can resolve a maximum of 10 IPv4 addresses and 10 IPv6 addresses (for a total maximum of 20 address objects) per FQDN. In PAN-OS 7.0 and later releases, you can now resolve a maximum of 64 addresses (32 of each) per FQDN address object. There is a Known Issue (PAN-59614 (98576)) where the number of addresses you can successfully resolve is limited to a combination of address types (IPv4 and IPv6) that does not exceed a total of 512B (the current DNS server response packet size).

Policy Features

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

VPN Features

New VPN Feature	Description
IKEv2 Support for VPN Tunnels	Site-to-site IPSec VPN is enhanced to support internet Key Exchange Version 2 (IKEv2), in addition to IKEv1 (the GlobalProtect agent is not included in this feature support). IKEv2: • Exchanges fewer messages than IKEv1 when setting up the tunnel endpoints. • Can negotiate multiple sets of traffic selectors to control which traffic can access the tunnel. • Provides a liveness check to determine if a peer gateway and tunnel are still up. • Supports NAT Traversal. • Supports the Hash and URL certificate exchange, which reduces fragmentation. • Supports cookie validation of a connection if a threshold number of concurrent IKE SA sessions is exceeded, reducing the potential for DoS attacks.
IPv6 IPSec VPN Support	Site-to-site IPSec VPN now supports IPv6 site-to-site connections, which allows you to establish IKE and IPSec Security Associations (SAs) between IPv6 gateways.
IPSec VPN Enhancements	You can now use the web interface to enable, disable, restart, or refresh an IKE gateway or an IPSec VPN tunnel to simplify troubleshooting. This feature applies to IPv4 and IPv6 tunnels.

GlobalProtect Features

For information about new authentication features supported on GlobalProtect (Suite B cryptography and SSL/TLS service profiles), see Authentication Features.

New GlobalProtect Feature	Description
Disable Direct Access to Local Networks	You can now disable direct access to local networks so that users cannot send traffic to proxies or local resources while connected to a GlobalProtect VPN. For example, if a user establishes a GlobalProtect VPN tunnel while connected to a public hotspot or hotel Wi-Fi and this feature is enabled, all traffic is routed through the tunnel and is subject to policy enforcement by the firewall.
Static IP Address Allocation	An enhancement to the IP address allocation logic enables the GlobalProtect gateway to maintain an index of clients and IP addresses so that the endpoint automatically receives the same IP address for all subsequent GlobalProtect VPN connections. The gateway continues to issue IP addresses in a round-robin fashion until all IP addresses are exhausted. To ensure that an endpoint receives the same address and to avoid IP address conflicts, create an IP address pool large enough to accommodate the number of endpoints. Alternatively, you can now configure a GlobalProtect gateway to assign fixed IP addresses using an external authentication server. This is useful when downstream resources, such as printers, servers, and applications, use a fixed source IP address/IP address pool to allow access for a specific user, user group, or OS. When enabled, the GlobalProtect gateway allocates the IP address to connecting devices using the Framed-IP-attribute from the authentication server.
Apply a Gateway Configuration to Users, Groups, and/or Operating Systems	You can now specify one or more users or user groups and/or client operating systems to which to apply a remote user tunnel configuration. For example, by configuring different IP address pools and access routes for Windows-based clients or for users in user groups such as Engineering, you can ensure that each client receives the correct network settings.
Welcome Page Management	The GlobalProtect client configuration now includes a setting to force the Welcome Page to display each time a user initiates a connection. This prevents the user from dismissing important information such as terms and conditions that may be required by your organization to maintain compliance. Alternatively you can provide the user the ability to dismiss seeing the Welcome page at subsequent logins.
Remote Desktop Connection to a Remote Client	The GlobalProtect VPN tunnel functionality has been enhanced to allow users, such as IT Help Desk, to RDP to a client device when connected over GlobalProtect VPN enabling troubleshooting and support for remote Windows users. Now, when IT Help Desk personnel log in to a client device, the GlobalProtect app can detect a new login without bringing down the RDP tunnel. After the administrator logs into the remote machine and successfully authenticates with the gateway, the GlobalProtect app reassigns the RDP tunnel to the remote administrator. This security measure prevents unauthorized access to VPN resources because policy enforcement for traffic through the RDP tunnel is now enforced and logged based on the privileges of the RDP user.

New GlobalProtect Feature	Description
Simplified GlobalProtect License Structure	You can now use GlobalProtect to provide a secure, remote access or virtual private network (VPN) solution via single or multiple external gateways, without any GlobalProtect licenses. The portal license, which was required to enable this functionality, has been deprecated. However, advanced features that include Host Information Profile (HIP) checks and support for the GlobalProtect mobile app for iOS and Android still require a gateway subscription. To take advantage of the new license structure, you need to upgrade only the device running the GlobalProtect portal to a PAN-OS 7.0 or later release.

Licensing Features

New Licensing Feature	Description
Self-Service License & Subscription Management	The firewall and Panorama now provide the capability to unassign or deactivate the active licenses on a firewall and assign the licenses to another firewall. To release the active licenses attributed to a firewall, you now have two options: • Deactivate a feature license or subscription on a firewall—If you accidentally installed a license/subscription on a firewall and need to reassign the license to another firewall, you can deactivate an individual license and re-use the same authorization code on another firewall without help from Technical Support. This capability is supported on the CLI of both the hardware-based firewalls and the VM-Series firewalls. • Deactivate licenses on a VM-Series firewall—When you no longer need an instance of the VM-Series firewall, you can free up all active licenses—subscription licenses, VM-Capacity licenses, and support entitlements—using the web interface or CLI on the firewall or Panorama. The licenses are credited back to your account and you can use the same authorization codes on a different instance of the VM-Series firewall.
Support for Usage-Based Licensing in Amazon Web Services (AWS)	The VM-Series firewall in AWS now supports the usage-based pricing model, in addition to the Bring Your Own License (BYOL) model. This capability makes it easier to consolidate the billing of AWS resources and the usage fees for the VM-Series firewall. The usage-based model in the AWS Marketplace is available in hourly and annual pricing bundles: • VM-Series capacity license with the Threat Prevention license for each model—VM-100, VM-200, VM-300, or VM-1000-HV. It includes a premium support entitlement. • VM-Series capacity license with the complete suite of licenses, which includes Threat Prevention, GlobalProtect, WildFire, and PAN-DB URL Filtering capabilities for each model—VM-100, VM-200, VM-300, or VM-1000-HV. It includes a premium support entitlement. Usage-based subscriptions/licenses are handled automatically by AWS; these licenses cannot be activated on the firewall or managed from Panorama.
Term-Based Capacity Licenses on the VM-Series Firewall	A term-based license is a license that allows you to use the VM-Series firewall for a specified period of time. A term-based VM-Series capacity license will have an expiration date and the web interface will display renewal notifications before the license expires. If the capacity license expires, although the firewall will continue to operate at the licensed capacity, you cannot obtain software updates or content updates until you renew the capacity license.

Changes to Default Behavior

The following are changes to default behavior in PAN-OS 7.0:

> You can also see CLI Changes in PAN-OS 7.0 and XML API Changes in PAN-OS 7.0.

- ▲ Authentication Changes
- ▲ GlobalProtect Changes
- ▲ Management Changes
- ▲ Panorama Changes
- ▲ Threat Prevention Changes
- ▲ WildFire Changes

Authentication Changes

PAN-OS 7.0 has the following changes in default behavior for authentication features:

Feature	Change
RADIUS authentication	• RADIUS administrators can now log in to the firewall CLI as SSH users without first logging in to the web interface. • When sending authentication requests to a RADIUS server, PAN-OS and Panorama 7.0 and later releases always use the authentication profile name as the network access server (NAS) identifier, even if the profile is assigned to an authentication sequence. In pre-7.0 releases, the firewall and Panorama use the name of whichever authentication profile or sequence is configured for the service that initiates the authentication process (such as administrator authentication).

GlobalProtect Changes

PAN-OS 7.0 has the following changes in default behavior for GlobalProtect features:

Feature	Change
OTP Authentication	Previously, when a user logged in to a GlobalProtect gateway that was on the same firewall as the portal, the portal generated a short-lived gateway user authentication cookie (expired in 60 seconds). The gateway would use that cookie to authenticate the user without requiring the user to enter a second one-time password (OTP). This feature is now deprecated. To enable the same user experience, whereby the user is only required to enter an OTP once to connect to GlobalProtect, you must set the **Authentication Modifier** to **Cookie authentication for config refresh** when configuring the portal authentication behavior.
Portal licenses	The GlobalProtect portal license is now deprecated. Starting with the PAN-OS 7.0 release, you can use all GlobalProtect portal functionality (which was previously available) without installing an additional license. However, advanced features including Host Information Profile (HIP) checks and support for the GlobalProtect mobile app for iOS and Android still require a gateway subscription. To take advantage of the new license structure, you need to upgrade only the device running the GlobalProtect portal to a PAN-OS 7.0 or later release (the device running the GlobalProtect gateway can run PAN-OS 7.0 and earlier releases).

Management Changes

PAN-OS 7.0 has the following changes in default behavior for management features:

Feature	Change
Operational modes	FIPS mode is no longer supported in PAN-OS 7.0 and later releases. If your firewall is running a PAN-OS 6.1 or earlier release and is in FIPS mode, you must Enable FIPS and Common Criteria Support before you upgrade to a PAN-OS 7.0 or later release. Refer to the PAN-OS 7.0 Upgrade/Downgrade Considerations for more details.
DNS proxy	There is a change in the way virtual system reporting and server profiles make queries using DNS proxy. Previously, the firewall would send virtual system report queries and virtual system server profile queries to the DNS proxy that was specified for the firewall, even if there was a DNS proxy specified for the virtual system. Now, the virtual system report and virtual system server profile send their queries to the DNS server specified for the virtual system if there is one. If there is no DNS server specified for the virtual system, the DNS server specified for the firewall is queried. (The vsys-specific DNS server used is defined in **Device** > **Virtual Systems** > **General** > **DNS Proxy**.)
Tags	The maximum number of tags that the firewall and Panorama support is now increased from 2,500 to 10,000. This limit is enforced across the firewall/Panorama and is not allocated by virtual system or device group.

Feature	Change
Policy objects	When you clone an object or rule, the naming convention for the clone is now `<original-name>-<n>`, where `<original-name>` is the name of the original object or rule and <n> is a numeric suffix (starting at 1 for the first clone) that makes the clone name unique in its current scope (virtual system, device group, or Shared location). For example, if you twice clone a rule named Ingress-Traffic, the firewall names the first clone Ingress-Traffic-1 and names the second clone Ingress-Traffic-2.

Panorama Changes

PAN-OS 7.0 has the following changes in default behavior for Panorama features:

Feature	Change
Firewall licenses	Previously, to check for licensing changes to the managed firewalls, you had to manually click the **Refresh** button on the **Panorama** > **Device Deployment** > **Licenses** tab. Now, Panorama performs a daily check-in with the licensing server and retrieves license updates/renewals and pushes them to the managed firewalls. The daily check-in takes place between 1:00 am and 2:00 am, according to the **Time Zone** configured for Panorama (**Panorama** > **Setup** > **Management**).

Threat Prevention Changes

PAN-OS 7.0 has the following changes in default behavior for threat prevention features:

Feature	Change
Security profiles	The default actions for handling threats are now **alert** or **reset-both** (sides of the connection). In releases prior to PAN-OS 7.0, the defaults were **alert** or **block**. On upgrade, the **block** action will be converted to **reset-both** and the **drop-packets** option is now renamed as **drop**. On downgrade, all actions configured as **drop** or **reset** will be converted to **block**.

WildFire Changes

PAN-OS 7.0 has the following changes in default behavior for WildFire features:

Feature	Change
WildFire Analysis profile	File Blocking profiles with the action set to **forward** or **continue and forward** are migrated to the new WildFire Analysis profile in PAN-OS 7.0. To edit the migrated profiles or to create new profiles to forward files and email links for WildFire analysis, select **Objects** > **Security Profiles** > **WildFire Analysis**. Additionally, samples forwarded by the firewall for WildFire analysis are no longer added as entries to the Data Filtering logs (**Monitor** > **Data Filtering**); instead, use the CLI to verify that the firewall is forwarding samples. See the WildFire Analysis Profile for full details on this enhanced WildFire workflow.

CLI Changes in PAN-OS 7.0

The following table lists CLI commands that changed between PAN-OS 6.1 (orange text) and PAN-OS 7.0 (green text). The changes include command options that are deprecated or have new names, values, or command paths in PAN-OS 7.0.

PAN-OS 6.1 Commands	PAN-OS 7.0 Commands
Configuration Mode Commands	
`commit validate`	`validate [full | partial]`
`set deviceconfig setting wildfire cloud-server`	`set deviceconfig setting wildfire [public-cloud-server | private-cloud-server]`
`set deviceconfig setting ssl-decrypt [block-unknown-cert | block-timeout-cert]`	`set profiles decryption <name> ssl-forward-proxy [block-unknown-cert | block-timeout-cert]`
`set network ike crypto-profiles ike-crypto-profiles <name> lifetime days <value: 1-65535>`	`set network ike crypto-profiles ike-crypto-profiles <name> lifetime days <value: 1-365>`
`set network ike crypto-profiles ipsec-crypto-profiles <name> lifetime days <value: 1-65535>`	`set network ike crypto-profiles ipsec-crypto-profiles <name> lifetime days <value: 1-365>`
`set network tunnel global-protect-gateway <name> client ip-pool`	`set vsys <name> global-protect global-protect-gateway <name> remote-user-tunnel-configs <name> ip-pool`
`set network tunnel global-protect-gateway <name> client split-tunneling`	`set vsys <name> global-protect global-protect-gateway <name> remote-user-tunnel-configs <name> split-tunneling`
`set network dhcp interface <name> server option ippool-subnet`	`set network dhcp interface <name> server option subnet-mask`
`set [shared | vsys <name>] profiles virus <name> decoder <name> [action | wildfire-action] [block]`	`set [shared | vsys <name>] profiles virus <name> decoder <name> [action | wildfire-action] [reset-both]`
`set [shared | vsys <name>] profiles virus <name> application <name> action [block]`	`set [shared | vsys <name>] profiles virus <name> application <name> action [reset-both]`
`set [shared | vsys <name>] profiles [spyware | vulnerability] <name> rules action action [block]`	`set [shared | vsys <name>] profiles [spyware | vulnerability] <name> rules action action [reset-both]`
`set [shared | vsys <name>] profiles file-blocking <name> rules <name> action [forward | continue-and-forward]`	The `forward` and `continue-and-forward` options are deprecated. To forward files to WildFire, you must now configure a WildFire Analysis profile: `set profiles wildfire-analysis <name>`
`set [shared | vsys <name>] profiles [spyware | vulnerability] <name> threat-exception <threat-id> action [drop | drop-all-packets]`	In PAN-OS 7.0, the `drop` option performs the same action as the `drop-all-packets` option does in PAN-OS 6.1: `set [shared | vsys <name>] profiles spyware <name> threat-exception <threat-id> action drop`
`set reports <name> type url sortby user_agent`	The `user_agent` option is deprecated.
`set reports <name> type wildfire sortby filetype`	The `filetype` option is deprecated.
`set application-group <name> [<value1> | <value2> | …]`	`set application-group <name> members [<value1> | <value2> | …]`
`set scheduled <name> [non-recurring | recurring]`	`set scheduled <name> schedule-type [non-recurring | recurring]`
`set threats [spyware | vulnerability] <threat-id> default-action drop-packets`	`set threats [spyware | vulnerability] <threat-id> default-action drop`

PAN-OS 6.1 Commands	PAN-OS 7.0 Commands
set [shared | vsys <name>] authentication-sequence <name> lockout [failed-attempts | lockout-time]	The lockout options are deprecated for authentication sequences. You now set the failed log-in attempts limit and account lockout duration only for authentication profiles.
set [shared | vsys <name>] server-profile [ldap | radius] <name> domain	set [shared | vsys <name>] authentication-profile <name> user-domain
set [shared | vsys <name>] server-profile radius <name> checkgroup	set [shared | vsys <name>] authentication-profile <name> method radius checkgroup
set [shared | vsys <name>] server-profile radius <name> timeout <value: 1-30>	set [shared | vsys <name>] server-profile radius <name> timeout <value: 1-120>
set [shared | vsys <name>] server-profile radius <name> server <name> port <value: 0-65535>	set [shared | vsys <name>] server-profile radius <name> server <name> port <value: 1-65535>
set [shared | vsys <name>] server-profile kerberos <name> domain	set [shared | vsys <name>] authentication-profile <name> user-domain
set [shared | vsys <name>] server-profile kerberos <name> realm	set [shared | vsys <name>] authentication-profile <name> method kerberos realm
set [shared | vsys <name>] server-profile kerberos <name> server <name> port 0-65535	set [shared | vsys <name>] server-profile kerberos <name> server <name> port 1-65535
set [shared | vsys <name>] certificate <name> [display-common-name | display-subject | display-issuer]	The display-common-name, display-subject, and display-issuer options are deprecated. ⚠ To generate certificates, always use the request certificate generate operational command (instead of the set [shared | vsys <name>] certificate command).
set [vsys <name>] captive-portal server-certificate	set [vsys <name>] captive-portal ssl-tls-service-profile
set [vsys <name>] url-admin-override server-certificate	set [vsys <name>] url-admin-override ssl-tls-service-profile
set [vsys <name>] global-protect global-protect-portal <name> portal-config server-certificate	set [vsys <name>] global-protect global-protect-portal <name> portal-config ssl-tls-service-profile
set [vsys <name>] global-protect global-protect-gateway <name> server-certificate	set [vsys <name>] global-protect global-protect-gateway <name> ssl-tls-service-profile
Operational Mode Commands	
clear session id <value> <value: 1-2147483648>	clear session id <value> <value: 1-4294967295>
show session id <value> <value: 1-2147483648>	show session id <value> <value: 1-4294967295>
delete user-file	delete authentication user-file
delete software image	The image option is deprecated. The version option is not new but performs the same function as the image option: delete software version
request system software install file	The file option is deprecated. The version option is not new but performs the same function as the file option: request system software install version
request system software install load-config <value> file	The file option is deprecated. The version option is not new but performs the same function as the file option: request system software install load-config <value> version
delete radius-user	The radius-user option is deprecated.

PAN-OS 6.1 Commands	PAN-OS 7.0 Commands
`show user ip-user-mapping all type [NTLM | SSL/VPN]`	The `SSL/VPN` and `NTLM` options are deprecated. The new `SSO` (single sign-on) option is for both NTLM and Kerberos SSO: `show user ip-user-mapping all type SSO`
`show user ip-user-mapping all option [count | detail] type [NTLM | SSL/VPN]`	The `SSL/VPN` and `NTLM` options are deprecated. The new `SSO` (single sign-on) option is for both NTLM and Kerberos SSO: `show user ip-user-mapping all option [count | detail] type SSO`
`show user ip-user-mapping-mp all option [count | detail] no-group-only [no | yes] type [NTLM | SSL/VPN]`	The `SSL/VPN` and `NTLM` options are deprecated. The new `SSO` (single sign-on) option is for both NTLM and Kerberos SSO: `show user ip-user-mapping-mp all option [count | detail] no-group-only [no | yes] type SSO`
`show user email-lookup [base | bind-dn | bind-password | domain | group-object | name-attribute | proxy-agent | proxy-agent-port | use-ssl | mail-attribute | server | server-port]`	All the `email-lookup` options are deprecated except the `email` option. The following command is not new but has similar options: `show user group-selection [base | bind-dn | bind-password | group-object | name-attribute | proxy-agent | proxy-agent-port | use-ssl | server | server-port]`
`show log traffic session_end_reason`	`show log traffic session-end-reason`
`show log [threat | url | data] action [equal | not-equal] drop-all-packets`	`show log [threat | url | data] action [equal | not-equal] drop-all`
`debug software restart <process>`	`debug software restart [core | process] <process>`
`debug authd`	`debug authentication`
`debug authd [admin-db | use-domain]`	The `admin-db` and `use-domain` options are deprecated.
`debug device-server pan-url-db [cloud-static-list-enable | cloud-static-list-disable]`	The following configure mode command replaces the `cloud-static-list-enable` and `cloud-static-list-disable` options: `set deviceconfig setting pan-url-db cloud-static-list`
`debug dataplane packet-diag clear filter-marked-session id <value: 1-2147483648>`	`debug dataplane packet-diag clear filter-marked-session id <value: 1-4294967295>`
`debug user-id test ntlm-login`	The `ntlm-login` option is deprecated. The new `sso-login` (single sign-on) option is for both NTLM and Kerberos SSO: `debug user-id test sso-login`
`set management-server unlock`	`request authentication [unlock-admin | unlock-user]`
`request certificate generate nbits`	`request certificate generate certificate-name <value> <name> <value> algorithm [ECDSA | RSA] [ecdsa-nbits | rca-nbits]`

XML API Changes in PAN-OS 7.0

The PAN-OS 7.0 XML API has the following changes:

Feature	Change
Custom reports	On PA-7000 Series firewalls and Panorama, API requests for custom reports no longer support the synchronous (`asynch=no`) option. API requests now provide a job ID, which you can use to retrieve the report. Additionally, API requests for reports (`type=report`) are now processed asynchronously by default on all firewall platforms.

Commits and validation	• You can now fully or partially validate your configuration on the firewall or Panorama. The change in the XML API syntax is as follows:
	  ◦ PAN-OS 6.1 and earlier releases:
	`/api/?type=op&cmd=<commit><validate></validate></commit>`
	  ◦ PAN-OS 7.0 and later releases:
	`/api/?type=op&cmd=<validate><full></full></validate>`, and
	`/api/?type=op&cmd=<validate><partial>…</partial></validate>`
	• The XML document format to commit shared policies to device groups on Panorama using the PAN-OS XML API has changed in PAN-OS 7.0. This change is due to an enhancement to permit a commit to devices within the device group: the device group name is now an attribute node instead of a text node.
	The change in the XML API request is as follows:
	  ◦ PAN-OS 6.1 and earlier releases:
	`/api/?type=commit&action=all&cmd=<commit-all><shared-policy><device-group><name>DeviceGroupName</name></device-group></shared-policy></commit-all>`
	  ◦ PAN-OS 7.0 and later releases:
	`/api/?type=commit&action=all&cmd=<commit-all><shared-policy><device-group><entryname='DeviceGroupName'/></device-group></shared-policy></commit-all>`

Associated Software Versions

The following minimum software versions are supported with PAN-OS 7.0. To see a list of the next-gen firewall models that support PAN-OS 7.0, see the Palo Alto Networks® Compatibility Matrix.

Palo Alto Networks Software	Minimum Supported Version with PAN-OS 7.0
Panorama	7.0.1
User-ID Agent	6.0.0
Terminal Server Agent	6.0.0
NetConnect	Not supported with PAN-OS 7.0
GlobalProtect Agent	2.2.0
GlobalProtect Mobile Security Manager	6.1.0
Content Release Version	497

Known Issues

The following list describes WildFire Known Issues, GlobalProtect Known Issues, and Firewall and Panorama Known Issues in the PAN-OS 7.0 release:

> Starting with PAN-OS 7.0.11, these release notes identify all unresolved known issues using new issue IDs that include a product-specific prefix. Known issues for earlier releases use both their new issue IDs and their original issue IDs (in parentheses).
>
> For recent updates to known issues for a given PAN-OS release, refer to https://live.paloaltonetworks.com/t5/Articles/Critical-Issues-Addressed-in-PAN-OS-Releases/ta-p/52882.

Issue ID	Description
WildFire Known Issues	
WF500-1907 (77299) This issue is now resolved. See PAN-OS 7.0.3 Addressed Issues.	When using a Firefox browser to access the firewall web interface, WildFire Analysis reports do not show the Coverage Status for the sample, even when a signature is generated to identify the sample (**Monitor** > **Logs** > **WildFire Submissions** > **Detailed Log View** > **WildFire Analysis Report**). **Workaround**: To view the correct Coverage Status for a sample, use Chrome or internet Explorer browsers to access **WildFire Submissions** logs on the firewall web interface.
WF500-1584 (67624)	When using a web browser to view a WildFire Analysis Report from a firewall that is using a WF-500 appliance for file sample analysis, the report may not appear until the browser downloads the WF-500 certificate. This issue occurs after upgrading a firewall and the WF-500 appliance to a PAN-OS 6.1 or later release. **Workaround**: Browse to the IP address or hostname of the WF-500 appliance, which will temporarily download the certificate into the browser. For example, if the IP address of the WF-500 appliance is 10.3.4.99, open a browser and enter `https://10.3.4.99`. You can then access the report from the firewall by selecting **Monitor** > **WildFire Submissions**, clicking the log details icon, and then selecting the **WildFire Analysis Report** tab.
GlobalProtect Known Issues	
GPC-1941 (66745)	On managed mobile devices running iOS 8, unenrolling the device does not always remove the VPN profile and the Mobile Security Manager profile.
GPC-1737 (61720)	By default, the GlobalProtect app adds a route on iOS mobile devices that causes traffic to the GP-100 GlobalProtect Mobile Security Manager to bypass the VPN tunnel. **Workaround**: To configure the GlobalProtect app on iOS mobile devices to route all traffic—including traffic to the GP-100 GlobalProtect Mobile Security Manager—to pass through the VPN tunnel, perform the following tasks on the firewall hosting the GlobalProtect gateway (**Network** > **GlobalProtect** > **Gateways** > **Client Configuration** > **Network Settings > Access Route**): • Add `0.0.0.0/0` as an access route. • Enter the IP address for the GlobalProtect Mobile Security Manager as an additional access route.
Firewall and Panorama Known Issues	
PAN-77595	PA-7000 Series firewalls forward a SIP INVITE based on route lookup instead of Policy-Based Forwarding (PBF) policy.

Issue ID	Description
PAN-77237	Using the `debug skip-condor-reports no` CLI command to force Panorama 8.0 to query PA-7000 Series firewalls causes PA-7000 Series firewalls running a PAN-OS 7.0 release to reboot. Do not use this command if you use Panorama 8.0 to manage a PA-7000 Series firewall that is running a PAN-OS 7.0 release.
PAN-76162	Panorama 8.0 fails to query PA-7000 Series firewalls running a PAN-OS 7.0 release. ⚠ Do not use the `debug skip-condor-reports no` command to work around this issue if you use Panorama 8.0 to manage a PA-7000 Series firewall that is running a PAN-OS 7.0 release (known issue PAN-77237).
PAN-75881	Establishing a TCP session, then installing a content update, and then installing an Antivirus or WildFire update causes the firewall to discard, use wrong content, or fail to inspect and perform NAT for the session.
PAN-67072	In PAN-OS 6.1 and 7.0, the firewall applies the wrong security policy if a user attempts to download a blocked file by selecting **Resume** in the blocked page dialog presented by the browser, allowing the user to download the blocked file. This issue occurs when a security policy that blocks downloads has a lower priority than a security policy that applies an action such as URL filtering (but does not block downloads) on the same traffic. This issue is resolved in PAN-OS 7.1 and later releases. **Workaround:** Change the order of the security policies so that the download-blocking policy has a higher priority than the URL-filtering policy.
PAN-62453 (102159)	Entering vSphere maintenance mode on a VM-Series firewall without first shutting down the Guest OS for the agent VMs causes the firewall to shut down abruptly, and results in issues after the firewall is powered on again. Refer to Issue 1332563 in the VMware release notes: www.vmware.com/support/pubs/nsx_pubs.html **Workaround:** VM-Series firewalls are Service Virtual Machines (SVMs) pinned to ESXi hosts and should not be migrated. Before you enter vSphere maintenance mode, use the VMware tools to ensure a graceful shutdown of the VM-Series firewall.
PAN-61724 (101293)	The **Network Monitor** report (**Monitor > App Scope > Network Monitor**) displays only partial data when you select **Source** or **Destination** for a data set that includes a large number of source or destination IP addresses and usernames. However, the report does display all data as expected when you instead select **Application** or **Application Category** for a large data set.
PAN-61267 (100700)	If you plan to configure the GlobalProtect portal on an interface assigned to a virtual router that is part of a virtual router chain in the same zone, you must configure the portal on the first ingress interface in the VR chain. This is because the session is established when the packet ingresses the interface on the first virtual router. When it ingresses the second virtual router, because it is in the same zone and it matches an existing session, a second security lookup is not performed and the packet is therefore not routed to the proper port on the portal interface.
PAN-59636 (98602) This issue is now resolved. See PAN-OS 7.0.10 Addressed Issues.	The Panorama management server has a memory increase due to syncing of WildFire reports from Panorama to log collectors.
PAN-59614 (98576)	In PAN-OS 7.0 and later releases, the maximum number of address objects you can resolve for an FQDN is increased from 10 of each address type (IPv4 and IPv6) to a maximum of 32 each. However, the combination of IPv4 and IPv6 addresses cannot exceed 512B; if it does, addresses that are not included in the first 512B are dropped and not resolved.

Issue ID	Description
PAN-59258 (98112) This issue is now resolved. See PAN-OS 7.0.9 Addressed Issues.	For a firewall in an HA active/active configuration, session timeouts for some traffic unexpectedly refresh after a commit or HA sync attempt.
PAN-59037 (97806)	For firewalls running PAN-OS 7.0.7 in an HA active/active configuration, the peer that is not the session owner intermittently incorrectly ages out sessions, which results in the premature removal of those sessions from both peers.
PAN-58872 (97584)	The automatic license deactivation workflow for firewalls with direct internet access does not work. **Workaround**: Use the `request license deactivate key features <name> mode manual` CLI command to Deactivate a Feature License or Subscription Using the CLI. To Deactivate a VM, choose **Complete Manually** (instead of **Continue**) and follow the steps to manually deactivate the VM.
PAN-57471 (95611)	There is a caching issue with the management plane that results in WildFire reports and alerts for files that are already uploaded at least once to the firewall and that are followed by a configuration change or threat content update on the firewall that specifically blocks those same files.
PAN-57218 (95260)	The `pan-comm` option for restarting the dataplane communication process is not available in the `debug software restart process` operational CLI command.
PAN-55437 (92423)	High availability (HA) for VM-Series firewalls does not work in AWS regions that do not support the signature version 2 signing process for EC2 API calls. Unsupported regions include AWS EU (Frankfurt) and Korea (Seoul).
PAN-54806 (91395)	Simultaneous transfer of large files from two different SMB servers over a GlobalProtect connection from a Windows 8 endpoint causes the connection to fail. **Workaround:** In PAN-OS 7.0.8 and later releases, enable Heuristics on Windows 8 endpoints or set the tunnel interface MTU size to 1,300 to avoid this issue.
PAN-54611 (91086) This issue is now resolved. See PAN-OS 7.0.10 Addressed Issues.	There is an issue where the firewall experiences BGP disconnections because the firewall fails to send keepalive messages to neighbors within specified timers.
PAN-54604 (91075) This issue is now resolved. See PAN-OS 7.0.7 Addressed Issues.	If you configure LSVPN tunnel interfaces between a GlobalProtect LSVPN gateway and an LSVPN satellite, you cannot upgrade the LSVPN satellite to a PAN-OS 7.0 release while the LSVPN gateway continues to run a PAN-OS 6.1 or earlier release; if you do, the LSVPN tunnels no longer pass traffic as expected due to changes made to the encryption algorithm names when introducing Suite B ciphers in PAN-OS 7.0. **Workaround**: Upgrade both firewalls to PAN-OS 7.0 or a later release. If you cannot upgrade the LSVPN gateway to PAN-OS 7.0 or a later release, then upgrade the LSVPN satellite to PAN-OS 7.0.7 or a later release (or to a PAN-OS 7.1 release) to avoid this issue.
PAN-54153 (90326) This issue is now resolved. See PAN-OS 7.0.8 Addressed Issues.	The botnet log cleanup job on a PA-7000 Series firewall runs two hours before the system-generated botnet reports are triggered, which results in empty or no botnet reports when no logs are collected between jobs.

Issue ID	Description
PAN-54100 (90256) This issue is now resolved. See PAN-OS 7.0.8 Addressed Issues.	Decrypted SSH sessions are not mirrored to the decrypt mirror interface as expected.
PAN-53686 (89595)	Attempts to **Hide Panorama background header** (**Panorama** > **Setup** > **Operations** > **Custom Logos**) result in an error (`Edit breaks config validity`).
PAN-53550 (89385) This issue is now resolved. See PAN-OS 7.0.7 Addressed Issues.	For a firewall in an HA active/active configuration, session timeouts for some traffic unexpectedly refresh after a commit or HA sync attempt. ⚠ The fix for this issue introduced a known issue: PAN-59037 (97806).
PAN-52812 (88141)	Log in attempts on Panorama for administrators with an access-domain name longer than 31 characters will fail with the following error: `Login could not be completed. Please contact the administrator.` This is because the Access Domain field allows up to 63 characters but login operations allow a maximum of only 31 characters. **Workaround**: Ensure that the access-domain name for all administrators is no longer than 31 characters or upgrade to a PAN-OS 7.1 release, which allows the longer access-domain names (up to 63 characters).
PAN-52743 (88029)	If you have a system-wide firewall proxy configuration (**Device** > **Setup** > **Services**) in a PAN-OS 6.1 or earlier release and then upgrade to PAN-OS 7.0, the upgrade process will not automatically extend the proxy configuration to the WildFire public cloud, which includes a separate proxy configuration (**Device** > **Setup** > **WildFire**) in PAN-OS 7.0. **Workaround:** After you upgrade a firewall to PAN-OS 7.0, add the necessary proxy configuration for accessing the WildFire public cloud (**Device** > **Setup** > **WildFire**).
PAN-51943 (86623) This issue is now resolved. See PAN-OS 7.0.8 Addressed Issues.	A firewall in an HA active/passive configuration with an established FTP session drops FTP PORT command packets after a failover.
PAN-51181 (85397)	A Palo Alto Networks firewall, M-100 appliance, or WF-500 appliance configured to use FIPS operational mode will fail to boot when rebooting after an upgrade to a PAN-OS 7.0 release. **Workaround**: Enable FIPS and Common Criteria support on any Palo Alto Networks firewall or appliance before you upgrade to a PAN-OS 7.0 release.
PAN-50651 (84594)	On PA-7000 Series firewalls, one data port must be configured as a log card interface because the traffic and logging capabilities of this platform exceed the capabilities of the management port. A log card interface performs WildFire file-forwarding and log forwarding for syslog, email, and SNMP and these services require DNS support. If you 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`.

Issue ID	Description
PAN-50186 (83702) This issue is now resolved. See PAN-OS 7.0.6 Addressed Issues.	WildFire Analysis reports do not display as expected in the **WildFire Analysis Report** tab (**Monitor > Logs > WildFire Submissions > Detailed Log View**) on a PA-7000 Series firewall running PAN-OS 7.0.2 or later releases. **Workaround**: Use the WildFire portal (https://wildfire.paloaltonetworks.com) or the WildFire API to retrieve WildFire Analysis reports.
PAN-49708 (82849) This issue is now resolved. See PAN-OS 7.0.6 Addressed Issues.	A Panorama virtual appliance using a Network File System (NFS) storage partition incorrectly fails the file system integrity check for the NFS directory when rebooting Panorama after an upgrade to a Panorama 7.0 release.
PAN-49577 (82605) This issue is now resolved. See PAN-OS 7.0.4 Addressed Issues.	Offloaded policy-based forwarding (PBF) sessions will fail to egress a firewall running PAN-OS 6.1.4 and later releases if you **Enforce Symmetric Return** (**Policies** > **Policy Based Forwarding** > *<pbf-rule>* > **Forwarding**). **Workaround**: Disable **Enforce Symmetric Return** and create bidirectional PBF policies.
PAN-49399 (82299) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	There is a critical security vulnerability affecting PAN-OS 7.0.0. This issue specifically affects devices running PAN-OS 7.0.0 that are configured to use LDAP authentication for Captive Portal or for device management, including Panorama. This issue does not affect devices configured to use RADIUS or local authentication instead of LDAP authentication, nor does it affect any PAN-OS release other than PAN-OS 7.0.0. Due to the critical nature of this vulnerability, we strongly advise all customers who have installed PAN-OS 7.0.0 to upgrade as soon as possible to PAN-OS 7.0.1. Alternatively, you can downgrade to an older version of PAN-OS, such as PAN-OS 6.1 or PAN-OS 6.0.
PAN-49044 (81584) This issue is now resolved. See PAN-OS 7.0.3 Addressed Issues.	In Panorama 7.0, output from the `show ntp` command does not always display the correct NTP status. This primarily occurs when there is only one NTP server configured where, even when correctly connected to the NTP server, the `show ntp status` displays as `rejected`.
PAN-48933 (81373) This issue is now resolved. See PAN-OS 7.0.2 Addressed Issues.	When the firewall is configured to communicate with a WildFire cloud (public or private) through a proxy server, WildFire Analysis reports for samples analyzed in the WildFire public cloud are not displayed in the WildFire Submissions log (**Monitor** > **WildFire Submissions**). **Workaround**: Use the WildFire portal (https://wildfire.paloaltonetworks.com) or the WildFire API to retrieve WildFire Analysis reports.
PAN-48719 (80903) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	A PA-7050 firewall running a PAN-OS 6.1 or earlier release and managed by Panorama running PAN-OS 7.0.0 cannot accurately handle queries from Panorama. This results in the inability to display data in the Application Command Center (ACC) widgets and prevents log data from the PA-7050 firewall from being included in reports generated on Panorama.
PAN-48702 (80871) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	WildFire Analysis reports are not displayed for **WildFire Submissions** log entries when the firewall is configured to use a service route instead of the management interface to communicate with a WildFire cloud (public or private). **Workaround**: For firewalls running PAN-OS 7.0.1, you can retrieve WildFire Analysis reports through the WildFire portal (wildfire.paloaltonetworks.com) or the WildFire API. Additionally, you can specifically configure `wildfire.paloaltonetworks.com` as the WildFire public cloud to view integrated reports from within the web interface: • Web interface: select **Device** > **Setup** > **WildFire** > **General Settings**. • CLI: use the `set deviceconfig setting wildfire public-cloud-server wildfire.paloaltonetworks.com` command in configuration mode.

Issue ID	Description
PAN-48667 (80799) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	Files and email links sent using Simple Mail Transfer Protocol (SMTP) or Post Office Protocol version 3 (POP3) are not forwarded to the WildFire public cloud for analysis unless the firewall is also configured to forward files to a WildFire private cloud. For firewalls connected to a **WildFire Private Cloud**, forwarding to both the WildFire public cloud and WildFire private cloud works correctly (**Device** > **Setup** > **WildFire**).
PAN-48647 (80750)	When specifying the device group and template for the VM-Series NSX edition firewall, you cannot select a template stack or a descendant device group defined in a device group hierarchy on Panorama. You can assign the firewalls to a template and a parent device group only.
PAN-48565 (80589)	The VM-Series firewall on Citrix SDX does not support jumbo frames.
PAN-48550 (80561) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	Software forwarding of Layer 3 multicast traffic with Protocol Independent Multicast (PIM) does not function correctly.
PAN-48463 (80398) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	If you configure the firewall to use client certificates to authenticate administrators when they access the web interface and you enable Online Certificate Status Protocol (OCSP) verification, then the authentication will fail and administrators can't log in. **Workaround**: Clear the **Block session if certificate status is unknown** and **Block session if certificate status cannot be retrieved within timeout** check boxes in the certificate profile that the firewall uses to authenticate administrators.
PAN-48456 (80387)	IPv6-to-IPv6 Network Prefix Translation (NPTv6) is not supported when configured on a shared gateway.
PAN-48446 (80373) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	The options to **Clone** objects or policies in a shared gateway location and to **Move** objects or policies from a virtual system to a shared gateway location do not work correctly.
PAN-48421 (80323) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	On reboot, the link states for firewall interfaces do not come up. This issue occurs when you disable high availability (HA) on a firewall that was configured in HA and then reboot the firewall. **Workaround**: Use the `delete deviceconfig high-availability enabled` CLI command in configuration mode to delete the high availability configuration node.
PAN-48394 (80268) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	When switching to Common Criteria (CC) mode on a PA-7050 firewall running PAN-OS 7.0.0, the operation does not complete and shows the following error: `Set CCEAL4 Mode Sysd Error`. This issue occurs because the CC mode operation attempts to change the operational mode before the system process (*sysd*) is fully loaded. This operation sets the firewall to the factory default configuration without CC configuration changes. **Workaround**: Change to CC mode while running a PAN-OS 6.1 release before upgrading to PAN-OS 7.0.0.
PAN-48392 (80266) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	If you configure the PA-200, PA-500, or PA-2050 firewall to use a service route instead of the management (MGT) interface to connect to an LDAP server, the connection won't work and any firewall functions that rely on the connection will fail. **Workaround**: If you configured a service route before upgrading to a PAN-OS 7.0 release, reconfigure it as a destination service route or to set the **Source Interface** and **Source Address** fields of the service route (**Device** > **Setup** > **Services** > **Global** > **Service Route Configuration** > **IPv4** or **IPv6**) to **Use default**.

Issue ID	Description
PAN-48346 (80177)	The URL block page does not display as expected when proxied requests from client use CONNECT method.
PAN-47976 (79470 This issue is now resolved. See PAN-OS 7.0.2 Addressed Issues.	Panorama does not display WildFire Analysis reports correctly in the WildFire Submissions log. **Workaround**: In the **Context** drop-down, select the firewall that forwarded the log and display the report in the firewall context.
PAN-47969 (79462)	If you log in to Panorama as a Device Group and Template administrator and rename a device group, the **Panorama** > **Device Groups** page no longer displays any device groups. **Workaround**: After you rename a device group, perform a commit, log out, and log back in; the page then displays the device groups with the updated values.
PAN-47611 (78803) This issue is now resolved. See PAN-OS 7.0.2 Addressed Issues.	In Panorama, template settings that are global to every virtual system (vsys) on a firewall (for example, System log settings) can't reference configuration elements (for example, an Email server profile) that you add to a specific vsys instead of to the Shared location. Only template and device group settings that Panorama can push to a specific vsys (for example, Log Forwarding profiles) can reference elements that you add to a specific vsys. To create an element that both global and vsys-specific settings can reference, you must set the template **Mode** to **Multi VSYS** enabled and, when adding the element, set its **Location** to **Shared**.
PAN-47518 (78646) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	Firewalls incorrectly replace multibyte characters with a period character (.) when forwarding logs or event information to SNMP traps, to a syslog server, through email, or in scheduled log exports. This issue also occurs when exporting logs to CSV.
PAN-47073 (77850)	Web pages using the HTTP Strict Transport Security (HSTS) protocol sometimes do not display properly for end users. **Workaround**: End users should import an appropriate forward-proxy-certificate for their browsers.
PAN-47038 (77775) This issue is now resolved. See PAN-OS 7.0.2 Addressed Issues.	A validation error occurs when you try to move an object from its current device group to a destination device group that is lower in the hierarchy even if the policy rules or objects that reference the object are in the same destination or are in a device group that should inherit the object. **Workaround**: Clone the object to the destination.
PAN-46344 (76601)	When you use a Mac OS Safari browser, client certificates will not work for Captive Portal authentication. **Workaround**: On a Mac OS system, instruct end users to use a different browser (for example, Mozilla Firefox or Google Chrome).
PAN-45793 (75806)	In a firewall with multiple virtual systems, if you add an authentication profile to a virtual system and give the profile the same name as an authentication sequence in Shared, reference errors occur. The same errors occur if the profile is in Shared and the sequence with the same name is in a virtual system. **Workaround**: When creating authentication profiles and sequences, always enter unique names, regardless of their location. For existing authentication profiles and sequences with similar names, rename the ones that are currently assigned to configurations (for example, a GlobalProtect gateway) to ensure uniqueness.

Issue ID	Description
PAN-44901 (74423) This issue is now resolved. See PAN-OS 7.0.2 Addressed Issues.	When fetching a dynamic block list, a firewall running PAN-OS 7.0.1 incorrectly uses the URL Updates service route instead of the service route that is attached to the Palo Alto Updates in the service route configuration (**Device** > **Setup** > **Services** > **Global**).
PAN-44616 (73997)	On the **ACC** > **Network Activity** tab, if you add the label Unknown as a global filter, the filter gets added as A1 and query results display A1 instead of Unknown.
PAN-44400 (73674)	The link on a 1Gbps SFP port on a VM-Series firewall deployed on a Citrix SDX server does not come up when successive failovers are triggered. This behavior is only observed in an HA active/active configuration. **Workaround**: Use a 10Gbps SFP port instead of the 1Gbps SFP port on the VM-Series firewall deployed on a Citrix SDX server.
PAN-44300 (73518)	WildFire Analysis reports cannot be viewed on firewalls running PAN-OS 6.1 release versions if connected to a WF-500 appliance in Common Criteria mode that is running a PAN-OS 7.0 release.
PAN-43000 (71624)	Vulnerability detection of SSLv3 fails when SSL decryption is enabled. This can occur when you attach a Vulnerability Protection profile (that detects SSLv3-CVE-2014-3566) to a Security policy rule and that Security policy rule and an SSL Decryption policy rule are configured on the same virtual system in the same zone. After performing SSL decryption, the firewall sees decrypted data and no longer sees the SSL version number. In this case, the SSLv3 vulnerability is not identified. **Workaround**: SSL Decryption Enhancements were introduced in PAN-OS 7.0 that enable you to prohibit the inherently weaker SSL/TLS versions, which are more vulnerable to attacks. For example, you can use a Decryption profile to enforce a minimum protocol version of TLS 1.2 or select **Block sessions with unsupported versions** to disallow unsupported protocol versions (**Objects** > **Decryption Profile** > **SSL Decryption** > **SSL Forward Proxy** and/or **SSL Inbound Inspection**).
PAN-42141 (70335) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	When a tunnel monitor is enabled for a large scale VPN (LSVPN) and the tunnel monitor is in wait recover mode, access routes from the GlobalProtect gateway cannot be installed on the GlobalProtect satellite.
PAN-42058 (70222)	If the password for the administrator's account on the NSX Manager contains special characters (such as "$"), Panorama cannot communicate with the NSX Manager. The inability to communicate prevents context-based information, such as Dynamic Address Groups, from being available to Panorama. **Workaround**: Remove special characters from the password on the NSX Manager.
PAN-41558 (69458)	When you use a firewall loopback interface as a GlobalProtect gateway interface, traffic is not routed correctly for third-party IPSec clients, such as StrongSwan. **Workaround**: Use a physical firewall interface instead of a loopback firewall interface as the GlobalProtect gateway interface for third-party IPSec clients. Alternatively, configure the loopback interface that is used as the GlobalProtect gateway to be in the same zone as the physical ingress interface for third-party IPSec traffic.
PAN-40842 (68330)	When you configure a firewall to retrieve a WildFire signature package, the System log shows `unknown version` for the package. For example, after a scheduled WildFire package update, the system log shows: `Wildfire package upgraded from version <unknown version> to 38978-45470.` This is a cosmetic issue only and does not prevent the WildFire package from installing.

Issue ID	Description
PAN-40714 (68095)	If you access **Device** > **Log Settings** on a device running a PAN-OS 7.0 or later release and then use the CLI to downgrade the device to PAN-OS 6.1 or an earlier release and reboot, an error message appears the next time you access **Log Settings**. This occurs because PAN-OS 7.0 and later releases display **Log Settings** in a single page whereas PAN-OS 6.1 and earlier releases display the settings in multiple sub-pages. To clear the message, navigate to another page and return to any **Log Settings** sub-page. The error will not recur in subsequent sessions.
PAN-40501 (67713) This issue is now resolved. See PAN-OS 7.0.1 Addressed Issues.	PAN-OS allows downgrade to content release versions (Applications and Threats) on the firewall to versions that the current PAN-OS release does not support. For example, if the firewall is running PAN-OS 7.0.1 and the minimum content release version is 497, the administrator should not be able to downgrade to a version earlier than 497.
PAN-40429 (67552)	Firewalls running PAN-OS 6.0 and earlier releases send a NIL value ("–" or en-dash) to the syslog server when no domain or hostname value is configured on the firewall. In PAN-OS 6.1 and later releases, the firewall does not send any value when the domain and hostname fields are empty; instead, this field is left blank in syslog headers.
PAN-40130 (66976)	In the WildFire Submissions Logs, the email recipient address is not correctly mapped to a username when configuring mapping with group mapping profiles that are pushed in a Panorama template.
PAN-40079 (66887)	The VM-Series firewall on KVM, for all supported Linux distributions, does not support the Broadcom network adapters for PCI pass-through functionality.
PAN-40075 (66879)	The VM-Series firewall on KVM running on Ubuntu 12.04 LTS does not support PCI pass-through functionality.
PAN-39728 (66233)	The URL logging rate is reduced when HTTP header logging is enabled in the URL Filtering profile (**Objects** > **Security Profiles** > **URL Filtering** > **URL Filtering profile** > **Settings**).
PAN-39636 (66059)	Regardless of the **Time Frame** you specify for a scheduled custom report on a Panorama M-Series appliance, the earliest possible start date for the report data is effectively the date when you configured the report. For example, if you configure the report on the 15th of the month and set the **Time Frame** to **Last 30 Days**, the report that Panorama generates on the 16th will include only data from the 15th onward. This issue applies only to scheduled reports; on-demand reports include all data within the specified **Time Frame**. **Workaround**: To generate an on-demand report, click **Run Now** when you configure the custom report.
PAN-39501 (65824)	Unused NAT IP address pools are not cleared after a single commit, so a commit fails if the total cache of unused pools, existing used pools, and new pools exceed the memory limit. **Workaround**: Commit a second time, which clears the old pool allocation.
PAN-38584 (63962)	Configurations pushed from Panorama 6.1 and later releases to firewalls running PAN-OS 6.0.3 or earlier releases will fail to commit due to an unexpected `Rule Type` error. This issue is caused by the new **Rule Type** setting in security policy rules that was not included in the upgrade transform and, therefore, the new rule types are not recognized on devices running PAN-OS 6.0.3 or earlier releases. **Workaround**: Only upgrade Panorama to version 6.1 or later releases if you are also planning to upgrade all managed firewalls to a PAN-OS 6.0.4 or later release before pushing configuration to firewalls.
PAN-38255 (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.

Issue ID	Description
PAN-37511 (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.
PAN-37177 (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 firewall as a managed device. If you reboot Panorama without committing the changes, the firewall will not connect back to Panorama; although the device group will display the list of devices, the device will not display in **Panorama** > **Managed Devices**. Further, if Panorama is configured in an HA configuration, the VM-Series firewall is not added to the passive Panorama peer until the active Panorama peer synchronizes the configuration. During this time, the passive Panorama peer will log a critical message: `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 setup, the commit will initiate the synchronization of the running configuration between the Panorama peers.
PAN-37044 (59573)	Live migration of the VM-Series firewall is not supported when you enable SSL decryption using the SSL forward proxy method. Use SSL inbound inspection if you need support for live migration.
PAN-36730 (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.
PAN-36433 (58260)	If an HA failover occurs on Panorama at the time that the NSX Manager is deploying the VM-Series NSX edition firewall, the licensing process fails with the error: `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.
PAN-36409 (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.
PAN-31832 (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 an HA configuration, the display of information from the `show ha-status` and `show hsm info` commands is blocked for 20 seconds.
PAN-31593 (49322)	After you configure a Panorama M-Series appliance for HA and synchronize the configuration, the Log Collector of the passive peer cannot connect to the active peer until you reboot the passive peer.

Issue ID	Description
PAN-29441 (45464)	The Panorama virtual appliance does not write summary logs for traffic and threats as expected after you enter the `clear log` command. **Workaround**: **Reboot Panorama** management server (**Panorama** > **Setup** > **Operations**) to enable summary logs.
PAN-25743 (40436)	Firewalls running PAN-OS 6.1 and later releases do not update FQDN entries unless you enable the DNS proxy **Cache** option (**Network** > **DNS Proxy** > *<DNS Proxy config>* > **Advanced**).

PAN-OS 7.0.16 Addressed Issues

The following table lists issues that are addressed in the PAN-OS® 7.0.16 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review information about how to Upgrade to PAN-OS 7.0.

Starting with PAN-OS 7.0.11, 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 ID	Description
PAN-77033	Fixed an issue where using a Panorama management server running PAN-OS 8.0 to generate a report that queried an unsupported log field from a PA-7050 firewall running PAN-OS 7.1 slowed the performance of Panorama because the *mgmtsrvr* process stopped.
PAN-74613	Fixed an issue where the `show running url-cache statistics` CLI command did not display enough information to diagnose issues related to URL category resolution. With this fix, the error messages indicate what failed and the exact point of failure.
PAN-74655	Fixed an issue where users experienced slow network connectivity due to CPU utilization spikes in the firewall network processing cards (NPCs) when the URL cache exceeded one million entries.
PAN-75215	Fixed an issue where the active firewall in an HA deployment kept sessions active for an hour instead of discarding them after 90 seconds when the sessions matched the URL category in a policy rule that was set to deny.
PAN-46374	Fixed an issue on the PA-7050 firewall where the Switch Management Card (SMC) did not come up following a soft reboot (such as after upgrading the PAN-OS software); power cycling was required to bring up the SMC.
PAN-64928	Fixed an issue where a PA-3000 Series firewall did not come up after the first reboot following an upgrade; a second reboot was required to bring up the firewall.
PAN-62159	Fixed an issue where the firewall did not generate WildFire Submission logs when the number of cached logs exceeded storage resources on the firewall.
PAN-68543	A security-related fix was made to address OpenSSL vulnerabilities (CVE-2016-8610).
PAN-62500	A security-related fix was made to prevent the inappropriate disclosure of information due to a Linux Kernel vulnerability (CVE-2016-5696).

PAN-OS 7.0.15 Addressed Issues

The following table lists issues that are addressed in the PAN-OS® 7.0.15 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review information about how to Upgrade to PAN-OS 7.0.

Starting with PAN-OS 7.0.11, 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 ID	Description
PAN-74188	Fixed an issue where conflicting next-hop entries in the egress routing table caused the firewall to incorrectly route traffic that matched Policy-Based Forwarding (PBF) policy rules configured to **Enforce Symmetric Return**.
PAN-73914	A security-related fix was made to address OpenSSL vulnerabilities (CVE-2017-3731).
PAN-73045	Fixed an issue where HA failover and fail-back events terminated sessions that started before the failover.
PAN-72769	A security-related fix was made to prevent brute-force attacks on the GlobalProtect external interface (CVE-2017-7945).
PAN-70674	A security-related fix was made to prevent cross-site scripting (XSS) attacks through the GlobalProtect external interface (CVE-2017-7409).
PAN-70541	A security-related fix was made to address an information disclosure issue that was caused by a firewall that did not properly validate certain permissions when administrators accessed the web interface over the management (MGT) interface (CVE-2017-7644).
PAN-69801	Fixed an issue where firewalls that had an HA active/active configuration and where the primary peer was in a tentative HA state did not synchronize session update messages between the peers, which resulted in dropped session packets after a session aged out (within 30 seconds).
PAN-62015	Fixed an issue on PA-7000 Series firewalls where, when creating the key for a GRE packet, the firewall did not use the same default values for the source and destination ports in the hardware and software, which slowed the firewall performance.
PAN-60376	Fixed an issue where the authentication process (*authd*) stopped responding and caused the firewall to reboot after the firewall received a stale response to an authentication request before selecting CHAP or PAP as the protocol for authenticating to a RADIUS server.
PAN-58589	Fixed an issue where the dataplane restarted when an out-of-memory condition occurred on a process (*pan_comm*).
PAN-57520	Fixed an issue where firewalls stopped connecting to Panorama when the root CA server certificate on Panorama expired. With this fix, Panorama replaces the original certificate with a new certificate that expires in 2024.

Issue ID	Description
PAN-53116	Fixed an issue on firewalls with LACP enabled where a commit or LACP flapping caused a memory leak in the dataplane.
FPGA-232	Fixed an issue on PA-5000 Series firewalls where packets became stuck in the FPGA, which resulted in packet loss and, on HA firewalls with path monitoring configured, triggered a failover.

PAN-OS 7.0.14 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.14 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Starting with PAN-OS 7.0.11, 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 ID	Description
PAN-71892	Fixed an issue where an LDAP profile did not use the configured port; the profile used the default port, instead.
PAN-71073	Fixed an issue where a commit associated with a dynamic update caused an HA failover when the path-monitoring target IP address aged out or when the first path-monitoring health check failed.
PAN-68431	Fixed an issue where firewalls and Panorama failed to send SNMPv3 traps if you configured the service route to forward the traps over a dataplane interface.
PAN-68074	A security-related fix was made to address CVE-2016-5195 (PAN-SA-2017-0003).
PAN-67090	Fixed an issue where the web interface displayed an obsolete flag for the nation of Myanmar.
PAN-62319	Fixed an issue where multicast entries were pointing to the wrong IP address for a rendezvous point (RP) because a recycled interface ID allocated for PIM register encapsulation retained an old tunnel interface that pointed to the wrong RP.
PAN-59654	Fixed an issue where commits failed on the firewall after upgrading from a PAN-OS 6.1 release due to incorrect settings for the HexaTech VPN application on the firewall. With this fix, upgrading from a PAN-OS 6.1 release to a PAN-OS 7.0.14 or later release does not cause commit failures related to these settings.
PAN-58496	Fixed an issue where custom reports using threat summary were not populated.
PAN-56684	Fixed an issue where DNS proxy static entries stopped working when there were duplicate entries in the configuration.

PAN-OS 7.0.13 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.13 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Starting with PAN-OS 7.0.11, 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 ID	Description
PAN-72616	Fixed an issue on PA-7000 Series firewalls where sessions were dropped with the `flow_bind_pending_full` message when using Ethernet IP (etherip) protocol 97, which resulted in unstable connections and delayed responses.
PAN-70428	A security-related fix was made to prevent inappropriate information disclosure to authenticated users (CVE-2017-5583 / PAN-SA-2017-0005).
PAN-70312	Fixed an issue where attempts to download threat packet captures (pcaps) from the threat logs failed with the error `File not found`, due to a missing Time Generated column.
PAN-68072	Fixed an issue on VM-Series firewalls where rebooting or configuring a new L3 interface caused the IP range configured on a disabled interface to be incorrectly installed in the FIB and routing table if you disabled the interface from the vSwitch.
PAN-68062	Fixed an issue where the firewall failed to apply the correct action if the vulnerability profile had a very long list of CVEs. With this fix, the firewall is able to support up to 64 CVEs per vulnerability rule. If the number of CVEs in the rule is more than 64, the firewall provides a warning on configuration commit.
PAN-67944	Fixed an issue where a process (*all_pktproc*) stopped responding because a race condition occurred when closing sessions.
PAN-66838	A security-related fix was made to address a Cross Site-Scripting (XSS) vulnerability on the management web interface (CVE-2017-5584 / PAN-SA-2017-0004).
PAN-64638	Fixed an issue where the firewall failed to send a RADIUS access request after changing the management interface's IP address.
PAN-63204	Fixed an issue where the firewall incorrectly assigned an expired User-ID IP mapping for 30 seconds after the original mapping had expired.
PAN-62822	Fixed an issue where the firewall dropped RTP traffic matching a predict session when a video call initiated from the external side of a shared gateway. With this fix, when a predict session goes across a different vsys or a shared gateway, the firewall uses the egress interface's vsys to lookup the destination zone instead of the session's vsys.
PAN-62074	Fixed an issue where the User-ID agent incorrectly read the IP address in the security logs for Kerberos login events.

Issue ID	Description
PAN-61837	Fixed an issue on PA-3000 Series and PA-5000 Series firewalls where the dataplane stopped responding when a session crossed vsys boundaries and could not find the correct egress port. This issue occurred when zone protection was enabled with a **SYN Cookies** action (**Network > Zone Protection > Flood Protection**).
PAN-60662	Fixed an issue on devices where commits failed due to issues with a process (*authd*).
PAN-60591	Fixed an issue where a custom role administrator with commit privileges could not commit configurations using the XML API.
PAN-59204	Fixed an issue where the firewall did not create an IPSec NAT-T session after a tunnel re-key until it originated a tunnel keep-alive. When this issue occurred, the firewall dropped NAT-T traffic packets.
PAN-57338	Fixed an issue where a slow file descriptor leak between two processes (*mgmtsrvr* and *pan_log_receiver*) caused the log receiver to stop responding and degraded management server performance. This issue occurred after a long device uptime of more than 380 days.
PAN-56839	Fixed an issue where the dataplane stopped responding when a change to the aggregate Ethernet (AE) link configuration was committed, resulting in an unexpected path monitoring condition.
PAN-56700	Fixed an issue where the SNMP OID `ifHCOutOctets` did not contain the expected data.
PAN-48095	Fixed an issue where the Panorama dynamic update schedule ignored the currently installed dynamic update version, and installed unnecessary dynamic updates.

PAN-OS 7.0.12 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.12 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Starting with PAN-OS 7.0.11, 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 ID	Description
PAN-69485	Fixed an issue where User-ID group mapping did not retain groups retrieved from Active Directory (AD) servers if there were any invalid groups in the group-mapping include list.
PAN-68045	Fixed an issue on PA-7000 Series firewalls where forwarding to WildFire failed due to an incorrect calculation of file size.
PAN-67986	Fixed an issue where the dataplane restarted due to a corruption in the QoS queue pointer.
PAN-67587	Fixed a rare condition where a dataplane process (*all_pktproc*) stopped responding.
PAN-67231	Fixed an issue on PA-5000 Series and PA-3000 Series firewalls where the dataplane restarted when processing traffic that had an incorrectly set IPv4 Reserved flag.
PAN-66540	Fixed an issue where the management interface and HA interfaces flapped during installation of a software upgrade, which caused HA failover or split brain.
PAN-64662	Fixed an issue where latency intermittently spiked over 3ms for IPsec traffic. With this fix, the conditions that contributed to latency spikes are addressed.
PAN-64368	Fixed an issue on PA-7000 Series firewalls where applying a Quality of Service (QoS) profile to an Aggregated Ethernet (AE) interface caused the reported maximum egress for the AE interface to differ from the sum of the egress values of the individual interfaces in the aggregate. With this fix, QoS statistics correctly report the configured QoS value of an AE interface.
PAN-64263	Fixed an issue where forward-proxy decryption failed if the server certificate record size exceeded 16KB.
PAN-63796	Fixed an issue on PA-7000 Series firewalls where internal looping of tunnel creation packets caused high dataplane CPU usage.
PAN-63142	Fixed an issue on firewalls where the dataplane restarted when processing IPv6 traffic that matched a predict session.
PAN-61534	Fixed an issue on the web interface where attempting to add multiple IP addresses to security policies (**Policies > Security**) failed with the error `range separator('-') not found -> Destination is invalid`.
PAN-61367	Fixed an issue where the firewall failed to send a TCP reset (RST) to the client-side and server-side devices when an application had a **Reset both** deny action in its security policy.

Issue ID	Description
PAN-61146	Fixed an issue where changing or refreshing an FQDN configuration with a large number of IP address entries (more than 32 IPv4 and IPv6 entries) in a single FQDN object caused the firewall or Panorama to stop responding.
PAN-60751	Fixed an issue where commit failed when an IKEv2 dynamic peer had the same proposal as an IKEv2 static peer with the same tunnel source interface. With this fix, a user is allowed to create one dynamic IKEv2 peer with the same proposal as a static peer, with both peers sharing the same tunnel interface.
PAN-60681	Fixed an issue where Panorama did not correctly verify Device group objects when pushing configurations with a large number of objects to firewalls, which caused commit failures with object validation errors.
PAN-60222	Fixed an issue where Panorama allowed you to configure a decryption type on **No Decrypt** policies. When Panorama pushed these policies to firewalls, it set the decryption type to the default value **SSL Forward Proxy**. With this fix, when you select **No Decrypt** as a policy rule action, Panorama disables configuration of the decryption type.
PAN-60182	In response to an issue where LACP flapped intermittently due to negotiation failures, priority for LACP processing is enhanced to mitigate flapping, and additional debug options are added to help isolate negotiation failures.
PAN-59411	Fixed an issue on firewalls where a process (*logrcvr*) stopped responding. With this fix, the process uses the correct buffer size to prevent the fault.
PAN-58516	Fixed an issue on PA-500 and PA-2000 Series firewalls where corruption of an instruction cache caused the firewall to restart. This issue occurred after the firewall was in continuous operation without a restart for hundreds of days.
PAN-58341	Fixed an issue where Panorama changed LDAP group mappings to `<ssl>no</ssl>`, which prevented end users from connecting when these mappings were pushed to devices. This issue occurred when upgrading from a PAN-OS 6.1 release to a PAN-OS 7.0 release.
PAN-57946	Fixed an issue on the M-100 appliance where a configuration for a subnet in the permitted IP addresses of interface Eth1 or Eth2 failed to take effect.
PAN-57819	Fixed an issue where disabling and importing local copies of Panorama policies and objects resulted in exclusion of Log Forwarding profile imports on multiple virtual systems (multi-vsys).
PAN-57787	Fixed an issue on Panorama where, if you used the CLI `replace` command to replace a device serial number, Panorama updated the managed device serial number but did not update the serial number in the deployment schedule and in custom reports.
PAN-57715	Fixed an issue where the firewall did not send all of the supported algorithms in the signature algorithm extension of `client hello` when negotiating connections with some SSL sites accessed from version 50 of the Chrome browser, which caused those connection attempts to fail.
PAN-57593	Fixed an issue where a decryption policy stopped decrypting SSL traffic if you enabled **Wait for URL** on SSL decryption.

Issue ID	Description
PAN-57145	Fixed an issue where, if the firewall performed IP and port NAT in the path of a GlobaProtect Large Scale VPN (LSVPN) IPSec tunnel, a re-key caused the firewall side to temporarily change back to the default port number for the new tunnel, and the intermediate NAT device dropped traffic until the old tunnel timed out or was deleted manually. With this fix, when a re-key happens, the firewall searches and applies the correct port number to the new tunnel immediately to prevent traffic drops.
PAN-57121	Fixed an issue where a VM-Series firewall that was in FIPS-CC mode could not connect to a Panorama server that was in normal mode.
PAN-56918	Fixed an issue where firewalls did not recognize malware that had been Base64-encoded in a zipped RTF file during an SMTP session.
PAN-56569	Fixed an issue where the top half of text lines failed to display correctly in the PDF version of the App Scope Threat Monitor Report (**Monitor > App Scope > Threat Monitor**).
PAN-56009	Fixed an issue on firewalls installed in an HA active/active configuration where out-of-order jumbo packets caused the dataplane to restart, which resulted in a failover.
PAN-55958	Fixed an issue where the firewall did not properly process active FTP data sessions if the FTP client reused—within a short period of time—the destination port number that was negotiated in the FTP control session.
PAN-55881	Fixed an issue on PA-5000 Series firewalls where the dataplane restarted in response to an out-of-memory condition. This issue occurred when a dataplane process stopped responding, and the information collection procedure that follows a process failure required more memory than what was available. With this fix, the information collection procedure does not run when a low-memory condition is present.
PAN-55737	Fixed an issue on PA-200 firewalls where, after the firewall rebooted and before NTP synchronization occurred, the firewall reported a reboot time without a timezone calculation to Panorama.
PAN-55243	Fixed an issue where an administrator with read-only privilege was unable to export Correlated Events logs in CSV format.
PAN-55190	Fixed an issue where firewalls failed to resolved URLs on the dataplane. This issue occurred when an out-of-memory error caused faults in the URL cache. With this fix, firewalls handle out-of-memory errors correctly, allowing proper resolution of URLs.
PAN-55045	Fixed an issue where adding objects such as tags to Panorama using the XML API resulted in those objects not being visible under **Policies**, **Addresses**, or **Services**.
PAN-54423	Fixed an issue where the firewall failed to make the CLI configuration **set authentication radius-vsa-on client-source-ip** persistent across system restart.
PAN-54279	Fixed an issue where the FTP file transfer of a large number of small files failed because the firewall did not install the FTP data-channel session in a timely manner.
PAN-53885	Fixed an issue where non-superuser administrators could not see exempt profiles and security policy rules when viewing threat details in a threat log.
PAN-52274	Fixed an issue where the User-ID process (*useridd*) stopped responding due to an issue in an internal library, which caused the firewall to reboot

Issue ID	Description
PAN-52177	Fixed an issue on PA-7000 Series firewalls where a newly installed and enabled Network Processing Card (NPC) did not have a correctly programmed forwarding table, which caused the firewall to drop packets until the forwarding table was manually flushed. With the fix, the firewall correctly programs the forwarding table upon slot startup.
PAN-52007	Fixed an issue where QoS statistics for a specific interface were empty after a device reboot.
PAN-49890	Fixed an issue where exporting custom reports to CSV, XML, and PDF failed.

PAN-OS 7.0.11 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.11 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Starting with PAN-OS 7.0.11, 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 ID	Description
PAN-66677	Fixed an issue on PA-5000 Series firewalls where traffic looped infinitely between dataplanes, which caused a loss of the affected traffic and a spike in CPU consumption.
PAN-66250	Fixed an issue on log collectors where a deadlock occurred for inter-log collector connections, which caused connectivity issues between log collectors and from firewalls to log collectors. This issue also caused local buffering of logs on the firewall. With this fix, log collector connection processing has been modified to eliminate this deadlock.
PAN-66210	Fixed an issue where a dataplane process failed to restart due to a missing or corrupt file, which caused the network processing card (NPC) to restart.
PAN-64360	Fixed an issue where the firewall failed to populate the email sender, recipient and subject information for WildFire reports.
PAN-63073	Security-related fixes were made to prevent denial of service attacks against the web management interface (PAN-SA-2016-0035).
PAN-62782	Fixed an issue where, if an LDAP refresh query terminated before completion, the firewall deleted users belonging to the domain user group in the active directory (AD).
PAN-62385	Fixed an issue where, if the firewall lost connectivity with an LDAP server or if you applied an invalid query filter, and these disruptions occurred during a User-ID group mapping update, the firewall deleted existing user-group mappings. With this fix, disruptions during a User-ID group mapping update will cause the firewall to stop adding new user-group mappings, and the firewall will not delete existing user-group mappings.
PAN-61815	Fixed a rare issue where VM-Series firewalls stopped generating traffic, threat or URL logs, or lost the ability to resolve the URL category.
PAN-61554	Fixed an issue on firewalls where a memory leak in a process (*authd*) caused all authentications to the firewall to fail.
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).s

Issue ID	Description
PAN-58673	Fixed an issue where the firewall did not use a second LDAP server for authentication if the first LDAP server was unreachable.
PAN-58418	Fixed an issue where Panorama could not sync to the NSX manager after a reboot or a failover, which caused a service outage. With this fix, sync works as expected.
PAN-58410	Fixed an issue on VM Series firewalls in an HA configuration where, after a failover occurred, an interface on the active firewall displayed its status as `ukn/ukn/down(autoneg)`.
PAN-58086	Fixed an issue on firewalls where a process (*devsrvr*) restarted if you committed a configuration that used more than 64 vendor IDs in a single vulnerability protection rule. With this fix, if you commit a configuration with more then 64 vendor IDs in a single rule, you receive a warning that you have exceeded the maximum number of IDs, and the process restart does not occur.
PAN-57855	Fixed an issue where the firewall stopped forwarding logs and discarded logs even when the incoming logging rate was low. With this fix, the processing of logs is optimized to increase prematching, and CPU load is reduced to prevent the queue from becoming full and discarding logs.
PAN-57323	Fixed an issue where VPN traffic went into a discard state because the firewall allowed packets to be sent through the tunnel prior to the completion of the IKE Phase 2 rekey process.
PAN-57055	Fixed an issue on VM-Series firewalls where traffic processing slowed down for two to three minutes after the firewall received a burst of packets on the HA2 data link.
PAN-56978	Fixed an issue where a VMware NSX edition firewall had incorrect address-group objects pushed via Panorama updates.
PAN-56973	Fixed an issue on firewalls where emails configured to use the per-virtual system (vsys) SMTP service route were sent using the global SMTP service route settings. With this fix, emails use the configured virtual system SMTP service route.
PAN-56775	Fixed an issue on firewalls where, if you configured the firewall to perform a monthly update of the external block list (EBL), the firewall incorrectly initiated an EBL refresh job every second.
PAN-56650	Fixed an issue where a log collector failed to send the system log to the active Panorama peer in an HA active/passive Panorama configuration after the active peer restarted.
PAN-56616	Fixed an issue where the firewall truncated user-group names when the name exceeded 150 characters. With this fix, the firewall preserves the complete group name even if the user-group name exceeds 150 characters, up to a maximum of 255 characters.
PAN-56438	Fixed an issue on firewalls where the internal value for block time in the Denial of Service (DoS) table exceeded the configured block time. This issue occurred on firewalls installed in an HA configuration.
PAN-56332	Fixed an issue where commits on Panorama failed because a process (*cord*) stopped responding.

Issue ID	Description
PAN-56280	Fixed an issue where the firewall displayed the status of a 10G SFP+ virtual wire interface as `10000/full/up` when the configured state of the interface was `auto/auto/down`. This issue occurred when **Link State Pass Through** in **Network** > **Virtual Wires** was enabled.
PAN-56221	A security-related fix was made to address a cross-site scripting (XSS) condition in the web interface (PAN-SA-2016-0033).
PAN-56200	Fixed an issue where the firewall allowed access to the search engine's cached version of a web page even though the page belonged to a URL category blocked by a policy.
PAN-56034	Fixed an issue where WildFire platforms experienced nonresponsive processes and sudden restarts under certain clients' traffic conditions.
PAN-55651	Fixed an issue on firewalls where, regardless of the configured metric, OSPF preferred Type 2 external metrics over Type 1 external metrics.
PAN-55560	Fixed an issue on firewalls where a memory condition caused the dataplane to restart with the message `Dataplane is down: too many dataplane processes exited`.
PAN-55237	A security-related fix was made to address an XPath injection vulnerability in the web interface (PAN-SA-2016-0037).
PAN-55199	Fixed an issue where, if you used SNMP to check the status of a tunnel interface, the firewall provided incorrect information.
PAN-54696	Fixed an issue on firewalls where incorrect handling of selective-acknowledgment (SACK) packets caused a decrease in download speeds on SSL-decrypted traffic.
PAN-53039	Fixed an issue on firewalls where the SNMP `ifOperStatus` OID did not reflect state changes of the aggregate Ethernet (AE) interfaces in an LACP trunk configuration.
PAN-52901	Fixed an issue where the dataplane restarted and dataplane processes stopped responding when passing SSH traffic using SSH decryption.
PAN-52379	A security-related fix was made to address CVE-2015-5364 and 2015-5366 (PAN-SA-2016-0025).
PAN-52183	Fixed an issue where Panorama management servers running PAN-OS 7.0 or a later PAN-OS release failed to display or download reports received from firewalls running PAN-OS 6.1 or earlier releases.
PAN-52164	Fixed an issue where Traffic logs reported cumulative bytes for sessions with TCP port reuse, which caused custom reports to incorrectly report the byte count.
PAN-49397	Fixed an issue on firewalls where a process (*varrcvr*) stopped responding when you requested WildFire statistics after receiving an unexpected response code from the WildFire Cloud, such as an error response code during query or upload.
PAN-48508	Fixed an issue where the passive Panorama server in an HA configuration did not display application data in the Application Command Center (ACC) or in AppScope.

PAN-OS 7.0.10 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.10 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Issue ID	Description
102600	Fixed an issue on firewalls where, if you configured GlobalProtect to use certificate-based authentication, users on Chromebook endpoints received prompts to log on using username and password.
101406	Fixed an issue on firewalls where CPU utilization on the dataplane was higher than expected.
101089	Fixed an issue where a firewall incorrectly applied SSL decryption to traffic in a custom URL category. This issue occurred when the firewall inspected traffic between the client and an explicit HTTP proxy, and the client hello message did not contain server name information (SNI).
100129	Fixed an issue on firewalls in an HA active-passive pair where HA configuration sync failed. This issue occurred when configuration sync from the active firewall happened while the passive firewall was in a state where a local commit failed. With this fix, configuration sync from the active firewall overwrites the configuration on the passive firewall, and configuration sync succeeds.
100115	Fixed an issue on firewalls where the dataplane restarted while processing a chain of tunnel packets.
99918	Fixed an issue on firewalls where a process (*devsrvr*) restarted repeatedly due to a problem with the internal URL cache structure.
99818	Fixed an issue where the firewall did not provide a blocked page response if you accessed a blocked application over HTTPS.
PAN-60568 99786	A security-related change was made to address a version disclosure in GlobalProtect (PAN-SA-2016-0026).
99057	Fixed an issue on firewalls where, if you configured virtual routers with OSPF Type-5 external routes with non-zero forward addresses, the routing tables of some virtual routers did not contain the routes. With this fix, OSPF Type-5 external routes install as expected in the virtual routers.
98684	Fixed an issue on VM-Series firewalls where, if path monitoring for HA used IPv6 addressing, the firewall used the wrong IPv6 address and path monitoring checking failed.
98602	Fixed an issue where the Panorama management server had a memory increase due to syncing of WildFire reports from Panorama to log collectors.
98388	Fixed an issue where the firewall brought down a tunnel that terminated at an IKE gateway configured for dynamic IP addressing when the IP address of the gateway changed. With this fix, the firewall does not bring down a tunnel if the IKE gateway dynamic IP address changes.

Issue ID	Description
98188	Fixed an issue on firewalls where HA failover did not occur immediately after the control plane failed on the active firewall.
97466	Fixed an issue on firewalls where a TCP reassembly failure for a reused TCP session prevented users from accessing Windows Server 2012 sites and applications.
97282	Fixed an issue on PA-7000 Series firewalls where a slot stopped responding due to a memory condition.
97063	Fixed an issue on firewalls where User ID group mapping stopped working due to a race condition.
96800	Fixed an issue on firewalls where, if you monitored server status from the user interface, the connection state appeared to toggle between the connected and disconnected states even though the server remained connected. This issue occurred for servers with agentless user mapping when you selected **Enable Session** in **Device** > **User Identification** > **User Mapping** > **Palo Alto Networks User-ID Agent Setup** > **Server Monitor**.
96155	Fixed an issue on VM-Series firewalls where the passive firewall interface in an HA pair went down, even with Passive Link State set to `auto` in the HA configuration.
96082	Fixed an issue where the firewall responded to Microsoft network load balancing (MS-NLB) multicast packets by incorrectly sending the multicast address as the source address.
PAN-57659 95895	A security-related fix was made to address a cross-site scripting condition in the web interface (PAN-SA-2016-0031).
95864	Fixed an issue where the GlobalProtect portal did not negotiate encryption algorithms correctly, which caused errors on recent releases of browsers with newly available stricter checking enabled. After this fix, the portal negotiates the correct algorithms to eliminate browser errors.
95797	Fixed an issue on Panorama where, if you selected **Group HA Peers**, previously selected individual firewalls became unselected, leaving only the most recently selected firewalls as part of the grouping configuration.
95604	Fixed an issue where firewalls configured with OSPFv3 adjacency and AH authentication header profiles failed to establish full adjacency because the fragmented OSPFv3 packets failed the AH authentication check.
95034	Fixed an issue on firewalls where, if you used the XML API to redistribute User-ID mapping information, and the mapping used a timeout value of `NEVER`, the firewall incorrectly changed the timeout value to `3600`.
94853	Fixed an issue where Panorama incorrectly removed the LDAP domain field when it pushed a template configuration to a firewall running a PAN-OS 6.x release. This issue occurred in a configuration when Panorama used a PAN-OS 7.x release and firewalls used a mixture of PAN-OS 6.x and PAN-OS 7.x releases.
94615	Fixed an issue on 7000-Series firewalls where the designated Log Card interface did not transmit a gratuitous ARP upon failover, which caused connectivity issues with neighboring devices.
94435	Fixed an issue where a firewall failed to learn of OSPF neighbors that were on interfaces configured with a maximum transmission unit (MTU) of 9216 because the OSPF database exchange failed for jumbo packets.

Issue ID	Description
94282	Fixed an issue on PA-7000 Series firewalls configured as HA pairs where, after the active firewall failed over to become the passive firewall, the newly passive firewall restarted with the error message: `internal packet path monitoring failure`. With this fix, the firewall will not restart after becoming passive.
94166	Fixed an issue on firewalls where, if you configured a Netflow profile under a virtual system (vsys), you could not assign the Netflow profile to a sub-interface part of same vsys.
94136	Fixed an issue where a PA-200 firewall reported an antivirus update job as successful when the update downloaded without installing. With this fix, a larger timeout value allows the installation to complete.
94115	Fixed an issue on firewalls where, if you implemented an authorization profile for OSPF with MD5 authentication on a firewall configured for FIPS-CC mode, the dataplane restarted.
93770	Fixed an issue where the firewall interpreted a truncated external dynamic list IP address (such as 8.8.8.8/) as 0.0.0.0/0 and blocked all traffic. With this fix, the firewall ignores incorrectly formatted IP address entries.
93394	Fixed an issue on firewalls where the dataplane restarted when processing SSL packets with an oversized Layer 2 header.
92934	Fixed an issue where a firewall configured for DHCP relay (with multiple DHCP relays or in certain firewall virtual system configurations) rebroadcast a DHCP packet on the same interface that received the packet, which caused a broadcast storm. With this fix, the firewall drops duplicate broadcasts instead of retransmitting them.
92912	Fixed an issue on Panorama where an administrator received a `File not found` error when attempting to view a threat packet capture (pcap).
92701	Fixed an issue where Panorama displayed an `unauthorized request` message to a device-group and template administrator when the administrator attempted to view shared device group policies.
92621	Fixed an issue where forwarded threat logs used inconsistent formatting between the `Request` field and the `PanOSReferer` field. With this fix, the `PanOSReferer` field uses double quotes for consistency with the `Request` field.
92523	Fixed an issue where, for firewalls in an HA active/active configuration, an Oracle redirect's predict session synchronized to the peer device became stuck in the "Opening State" because the parent session was not installed on the peer device. With this fix, the firewall ensures the parent session is installed on the peer device and the Oracle redirect's predict session transitions to active state to allow for successful Oracle client-to-server communication.
91474	Fixed an issue that prevented a firewall in Common Criteria Evaluation Assurance Level 4 (EAL4) mode from connecting to Panorama HA pair units in Common Criteria (CC) mode.
91086	Fixed an issue where the firewall experienced BGP disconnections because the firewall failed to send keepalive messages to neighbors within specified timers.
90596	Fixed an issue on PA-5000 Series firewalls where the FPGA did not initialize. With this fix, the FPGA is automatically reprogrammed after an initialization failure so that it can attempt multiple reinitializations before triggering a boot failure.

Issue ID	Description
90508	Security-related fixes were made to address CVE-2016-0777 and CVE-2016-0778 (PAN-SA-2016-0011).
90145	Fixed an issue where the system log in Panorama did not contain complete username and job ID information. With this fix, Panorama displays the username and job ID correctly, but firewalls continue to show `panorama` as the username in system logs for commit-all configurations.
89891	Fixed an issue where Threat logs forwarded from the firewall had an extra colon when using TCP for the transport protocol. With this fix, the format of forwarded logs over TCP and UDP is consistent.
89284	Fixed a reporting issue where the non-standard port ACC widgets displayed inaccurate info. This issue occurred when traffic on the firewall ran on standard ports matching custom applications pushed by Panorama.
88841	Fixed an issue on firewalls where a process (*routed*) stopped responding.
88651	Fixed an issue where a process (*useridd*) stopped responding when the running-config was missing the port number associations for the Terminal Services (TS) Agent.
88194	Fixed an issue where Panorama did not log if the Force Template Values option was in the checked state when applying a Template or Device Group commit. With this fix, the Panorama logs will indicate if the Force Template Values option is in the checked state when doing a Template or Device Group commit.
87870	Fixed an issue where an OSPF route with a lower administrative distance than the static route should become the preferred route but was not installed and used as expected; the firewall continued to use the static route instead.
87727	Fixed an issue where a virtual system custom role administrator could not add user-to-IP mappings using the XML API.
87052	Fixed an issue where firewalls could not use an EU-region AWS virtual private cloud as a VM information source. This issue occurred because the firewall used signature version 2 to sign API requests while the EU-region Amazon Machine Image (AMI) used signature version 4. With this fix, the firewall uses the supported signature version.
85361	Fixed an issue where, if you used the CLI to input more than 126 addresses in an address group or 126 URLs in an allow-list, the firewall did not apply the configuration.
83569	Fixed an issue where multiple QoS changes while under a heavy load caused the dataplane to restart.
82165	Fixed an issue where a firewall configured to block URL categories over HTTPS did not send a FIN/ACK to the browser to close the connection after sending a block page. This issue occurred for firewalls configured to perform NAT.
81451	Fixed an issue on Panorama where device group and template administrators were unable to change their own passwords.
81178	Fixed an issue where, if you filtered the URL logs, the returned results did not include expected matches.
79472	Fixed an issue where Panorama truncated system logs to 180 characters.

PAN-OS 7.0.9 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.9 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Issue ID	Description
99505	Fixed an issue on firewalls where long client IDs caused the DHCP service to stop responding, leading to a firewall restart.
98510	Fixed an issue where exported log files did not correctly escape certain characters, such as commas (,), backslashes (\), and equal-to operators (=).
98327	Fixed an issue on firewalls where an FQDN refresh or a content update triggered an unexpected configuration commit after you applied a pre-commit validation. With this fix, an FQDN refresh or a content update will not trigger a configuration commit.
98112	Fixed an issue with firewalls in an HA active/active configuration where session timeouts for some traffic were unexpectedly refreshed after a commit or HA sync attempt.
97763	Fixed an issue where a PA-200 firewall failed to download a PAN-OS software update due to an incorrect disk space calculation.
97571	Fixed an issue on firewalls where eusing previous port information (tcp-reuse) for new sessions caused traffic in those sessions to be dropped.
97247	Fixed an issue where a PA-200 firewall failed to download a content update due to disk space issues after a failed antivirus update installation. With this fix, the firewall will, as part of the update installation process, clean up all temporary files even if the update installation fails.
97099	Fixed an issue where, after importing the configuration from a Panorama M-100 device to a Panorama M-500 device, the existing security profiles and log-forwarding profiles could not be selected.
95622	Security-related fixes were made to address issues identified in the May 3, 2016 OpenSSL security advisory (PAN-SA-2016-0020).
95462	Fixed an issue on PA-5000 and PA-7000 Series firewalls where the dataplane repeatedly stopped responding.
95133	Fixed an issue where firewall incorrectly applied policy-based forwarding (PBF) to sessions created via prediction (such as ftp-data sessions).
94765	Fixed an issue where NAT translation did not work as expected when the administrator deleted a virtual system (vsys) from a firewall with multiple virtual systems (multi-vsys) and NAT rules configured without first deleting NAT rules associated with the vsys. With this fix, when the administrator deletes a vsys, the firewall automatically deletes NAT rules associated with that vsys.
94573	Fixed an issue where, under specific conditions, a firewall dropped incoming PSH+ACK segments from the server.

Issue ID	Description
94569	Fixed an issue where integrated WildFire report from WF-500 did not display correctly when using Internet Explorer 11.
94165	Fixed an issue where the firewall generated WildFire Submissions logs with an incorrect email subject and sender information when sending more than one email to a recipient in a POP3 session.
93961	Fixed an issue where a process (*configd* or *mgmtsrvr*) restarted due to the use of special characters, such as a bracket character—"`[`" or "`]`"—in a search field (for example, in the "Address" section).
93865	Fixed an issue on an M-100 appliance in Log Collector mode where locally-created proxy configurations were lost when a commit was performed from Panorama. With this fix, locally-created proxy configurations persist after a Panorama commit.
93855	Fixed an issue where the DNS proxy template object that was pushed from Panorama did not override that object on the firewall as expected.
93783	Fixed an issue on firewalls where autocommit failed if an administrator configured an IPSec tunnel using the manual-key method.
93778	Fixed a rare issue where a bind request from the firewall to the LDAP server failed.
93667	Fixed an issue on firewalls where the GlobalProtect endpoint incorrectly failed the Host Information Profile (HIP) evaluation when there is an empty missing-patch tag in the HIP Report and the Check setting for patch management in HIP Objects criteria was set to **has-all** (**Objects** > **GlobalProtect** > **HIP Objects** > **Patch Management** > **Criteria**).
93540	Fixed an issue where a read-only superuser could not export a threat packet capture (PCAP) file from the GUI, which displayed a `File not found` message.
93531	Fixed an issue on firewalls where, if you exported to CSV format from two or more custom scheduled reports, the export process produced the same file for both reports.
93508	Fixed an issue where a process (*logrcvr*) stopped responding and restarted repeatedly after an upgrade to content release version 571, which caused the firewall to reboot. Content release version 572 mitigated this issue but this fix ensures that firewalls running PAN-OS 7.0.9 and later releases (or PAN-OS 7.1.2 and later releases) will not be affected by this issue.
93449	Fixed an issue where the API browser displayed the incorrect XML API syntax for the `show arp all` command.
92863	Fixed an issue where a process (*mgmtsrvr*) stopped responding and created core files during firewall startup.
92752	Fixed an issue where Panorama exported an incomplete CSV file because a custom report name contained a space.
92684	Fixed an issue on firewalls where a process (*l3svc*) stopped responding when processing a large number of user-authentication requests.
92677	Fixed an issue where the Comodo RSA certificate authority (CA) was not included in the default trusted root on the firewall, which caused SSL decryption to fail on sites using this as their CA.

Issue ID	Description
92610	Fixed an issue on PA-200 firewalls where the firewall stalled during boot-up after an upgrade from PAN-OS 6.1.12 or an earlier PAN-OS 6.1 release to a PAN-OS 7.0 or later release.
92472	Fixed an issue where, during the connection of a satellite to the GlobalProtect gateway, the Online Certificate Status Protocol (OCSP) verification for the GlobalProtect certificate failed because the OCSP response did not contain the signature certificate.
92466	Fixed an issue on Panorama where you could not enable the setting **remove tcp timestamp** in a zone protection profile pushed via a template from Panorama 7.0.x to devices running a PAN-OS 6.1 release. With this fix, Panorama will be able to push the **remove tcp timestamp** configuration to devices running a PAN-OS 6.1 release.
PAN-55259 92106	A security-related fix was made to address multiple NTP vulnerabilities (PAN-SA-2016-0019).
91998	Fixed an issue where the `set application dump on rule` CLI command did not work for Security policy rules pushed to firewalls from Panorama.
91785	Fixed an issue where a Panorama process (*configd*) stopped responding when trying to add tags to multiple firewalls (**Panorama > Managed Devices**) at the same time.
91522	Fixed an issue where a cloned application name could not be edited after it was cloned from a Shared/Device Group location to a Shared location. With this fix, the cloned application names are editable.
91379	Fixed an issue where an out-of-sequence packet was passed through the firewall.
91269	Fixed an issue where the firewall restarted the dataplane after a process stopped responding.
91156	Fixed an issue on Panorama where performing log queries and reports resulted in incorrect reporting of multiple Panorama logged-in administrators on PA-7000 Series firewalls.
91034	Fixed an issue on the WildFire platform where, if the snmp.log file was over 5MB, the SNMP daemon (*snmpd*) process cleared the log file and restarted.
90933	Fixed an issue where the firewall generated superfluous logs (for traffic that did not match the configured filters) after you enabled dataplane debugging. With this fix, the firewall will correctly filter the logs, but some superfluous logs will be observed.
90691	Fixed an issue on firewalls running a PAN-OS 7.0 or later release where the web interface became inaccessible (`502 bad gateway` error) when sending a high rate of concurrent User-ID XML API POST requests.
90677	Fixed an issue on firewalls where the *flow_mgmt* process stopped responding, which caused the dataplane to restart.
90618	Fixed an issue on Panorama where creating an exemption for a threat name from the Threat log caused the web interface to display the exemption multiple times depending on the number of sub-device groups. After the fix, the interface correctly displays only one profile name.
90252	Fixed an issue where firewalls deployed in an Active/Active configuration dropped DNS traffic packets with a corresponding increment in the `session_state_error` counter.

Issue ID	Description
90141	Improved output of the command request batch license info on Panorama to include license expiration times.
90106	Fixed an issue where a process restarted unexpectedly due to the reuse of a process ID (PID). The PID was associated with an old SSH session that the firewall intended to terminate because the SSH session had timed out but was never closed properly, which inadvertently resulted in a restart of the process currently associated with that PID.
89984	A security-related fix was made to address a stack overflow condition (PAN-SA-2016-0024).
89620	Fixed an issue where SSL inbound decryption failed when a client sent a ClientHello with TLS 1.2 while the server supported only TLS 1.0.
89264	Fixed an issue where DNS resolution failed when message compression was disabled on the DNS server, which resulted in case mismatch between CNAME query and answer values in DNS server replies. With this fix, the firewall ignores case in CNAME values so that query and answer values match and DNS requests resolve successfully.
88585	Fixed an issue where DNS proxy rules didn't consistently match a domain name with the correct primary IP addresses. With this fix, matching logic favors results that do not include wildcards.
88225	Fixed an issue where the firewall could not register with the WildFire public cloud due to a problem with the log-cache size becoming too large. With this fix, a limitation mechanism is added to control the log-cache size.
87414	Fixed a cosmetic issue where the `traffic` log type was displayed in the severity column of the Log Forwarding profile.
87223	Fixed an issue where a process (*mprelay*) stopped responding due to a race condition related to the age-out logic for MFIB entries.
87154	Fixed an issue where firewalls stopped forwarding data to the WildFire cloud. With this fix, if the connection to the WildFire cloud fails, the firewall attempts to reconnect after the initial failure and resumes forwarding when successfully reconnected.
86990	Fixed an issue on a firewall where a process (*sslvpn*) repeatedly restarted due to an internal thread synchronization issue.
86979	Fixed an issue where an incomplete IPSec tunnel configuration (one without an IKE gateway specified) caused the firewall server process to stop responding.
85015	Fixed an issue where the API did not list `Correlated Events` as supported log types. With this fix, the `type=log` parameter in the API includes `log-type=corr`, `log-type=corr-detail`, and `log-type=corr-categ` as supported log types. For more information, refer to Retrieve Logs (API).
83086	Fixed an issue where the output of the `show dos-protection <zone-name> blocked source` command didn't display the correct data for the requested zone.
83008	Fixed an issue where VM-Series firewalls experienced packet loss. With this fix, an internal buffer is increased in size to prevent the packet loss.

Issue ID	Description
82613	Fixed an issue where firewalls downloaded multiple Certificate Revocation Lists (CRLs) because the CRL verification process did not support certain extension types in the list. With this fix, if the firewall encounters a CRL with the extension `Issuing Distribution Point` it will return the status of the certificate as `Unknown`.
81750	Fixed an issue on PA-200 firewalls where files in the /tmp partition caused a low disk space condition. With this fix, some files in /tmp are relocated to other partitions to improve disk space allocation.
80628	Fixed an issue where WildFire content updates showed timestamps with future dates.
69900	Fixes introduced in PAN-OS 7.0.0 are enhanced in this release. With this fix in the PAN-OS 7.0.9 release, the tech support file contains a filtered version of the php.debug.log file, which was excluded from the previous fix.
44888	Fixed an issue on firewalls where, if you enabled SYN cookies, dropping the original SYN packet and sending SYN-ACK back to the client incorrectly triggered an increment in the `flow_dos_rule_drop` counter.

PAN-OS 7.0.8 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.8 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Issue ID	Description
97313	Fixed an issue where the management plane of Panorama M-100 and M-500 appliances stopped responding when renaming objects or security policies due to memory corruption.
96792	Fixed an issue where commits failed due to a memory leak related to HA sync of the candidate configuration that caused the passive Panorama peer to stop responding.
94757	Fixed a rare issue on firewalls where Security policy rules included empty dynamic block lists (0.0.0.0/0) after a **Commit** from Panorama with **Force Template Values** enabled.
93729	Fixed an issue where SSH decryption caused a dataplane memory leak and restart.
93072	A security-related change was made to address an issue in the policy configuration dialog (PAN-SA-2016-0014).
92763	Fixed an issue where commits failed due to a validation error that occurred when Panorama pushed Authentication Sequence profiles that included a virtual system that was not migrated properly during an upgrade from a Panorama 6.1 release to a Panorama 7.0 or later release.
92391	Fixed an issue where firewall Traffic logs displayed unusually large byte counts for sessions passing through proxy servers.
92293	A security-related fix was made to address CVE-2016-1712 (PAN-SA-2016-0012).
91900	Fixed an issue where a Panorama validate operation followed by an FQDN refresh caused the validated configuration change to commit to the firewall.
PAN-55122 91886	A security-related fix was made to address CVE-2015-7547 (PAN-SA-2016-0021).
91876	Fixed an issue where the passive firewall in a VM-Series ESXi configuration was processing and forwarding traffic.
91799	Fixed an issue were a PA-7050 firewall did not display logs as expected and caused a process (*logrcvr*) to stop responding.
91728	A security-related fix was made to address a Denial of Service condition related to the API (PAN-SA-2016-0008).
91724	Fixed an issue where an autocommit of an incremental antivirus update failed after a reload due to a corrupt virus signatures file and a failed incremental installation. With this fix, incremental content installation has enhanced protections to prevent autocommit failures, and will log additional information to assist with troubleshooting.
91653	Fixed an issue where SSL decryption did not work as expected for resumed sessions.

Issue ID	Description
91643	Fixed a rare issue where traffic that triggered an SSL decrypt URL proxy action caused a process (*all_task*) to restart.
91497	Fixed an issue where stale next-hop MAC entries persisted on the session offload processor after you modified a subinterface configuration, which caused SSH connections to fail. With this fix, the management plane cache no longer duplicates next-hop MAC entries, which prevents the stale entries that caused SSH connections to fail.
91336	Fixed an issue where the packet processor stopped responding when proxy packets were switched to the fast path group on the dataplane.
90982	Fixed an issue where upgrading from a PAN-OS 6.1 release to PAN-OS 7.0.3 or a later PAN-OS 7.0 release caused the GlobalProtect portal or gateway and SSL decryption processes to stop responding. This issue occurred because SSL/TLS Service Profiles (introduced in PAN-OS 7.0) were not created successfully if you did not enable multiple virtual system (multi-vsys) functionality on the firewall. With this fix, SSL/TLS Service profiles are now successfully created on non-multi-vsys platforms when upgrading to PAN-OS 7.0.8 or later releases or to PAN-OS 7.1 releases.
90857	Fixed an issue with a Panorama passive peer in an HA configuration where administrators were unable to configure the Dynamic Updates schedule for Applications and Threats updates.
90856	Fixed an issue where the dialog for creating certificates and the dialog for editing certificates had different character limits for the certificate name. With this fix, the certificate name field in both dialogs allows up to 63 characters.
90842	Fixed an issue where the firewall received an unencrypted empty ISAKMP packet in quick mode that caused a process (*ikemgr*) to stop responding.
90794	Fixed an issue where a log file (`/var/log/wtmp`) inflated and consumed the available disk space. With this fix, PAN-OS software uses a log rotation function to prevent log files from consuming more disk space than necessary.
90680	Fixed an issue on PA-500 firewalls where certain processes (*l3svc* and *sslvpn*) stopped responding after the firewall attempted a dynamic update.
90635	A security-related fix was made to address a cross-site scripting condition in the Application Command Center (ACC) (PAN-SA-2016-0009).
90553	Fixed an issue where Data Filtering and WildFire Submissions logs for non-NAT sessions contained incorrect or invalid NAT information.
90326	Fixed an issue on PA-7000 Series firewalls where botnet reports were not created consistently due to a log cleanup job that ran just prior to when the botnet reports were generated, which—on some days—resulted in empty or no botnet reports. With this fix, the botnet log cleanup job takes place after the daily generation of botnet reports so that daily reports are created and populated as expected.
90256	Fixed an issue where decrypted SSH sessions were not mirrored to the decrypt mirror interface as expected.
90249	Fixed an issue where upgrading from a PAN-OS 6.1 or earlier release prevented administrators from overriding LDAP group mappings that were pushed from Panorama.

Issue ID	Description
90044	Fixed an issue where log forwarding in Panorama failed when using syslog over TCP.
89979	Fixed an issue where the Aggregate Ethernet (AE) interface port in virtual wire mode with link state pass through enabled came up after a commit; although its peer AE interface port was down. With this fix, the other AE interface port will come up after the commit and is then brought down in approximately 10 seconds. This causes both AE interfaces to stay down until the first AE interface recovers.
89917	Fixed an intermittent issue where one or more interfaces on a VM-Series firewall deployed in the Amazon Web Services (AWS) cloud could not obtain IP addresses from a DHCP server after booting up.
89910	Fixed an issue where all LLDP packets were sent with the source MAC address of the MGT interface instead of the dataplane interface from which they were transmitted. With this fix, LLDP packets are encapsulated with the source MAC address of the interface that transmitted the packet.
89743	Fixed an issue where commits failed due to processes (*configd* and *mgmtsrvr*) that stopped responding. This issue was caused by memory corruption related to the scheduling of WildFire dynamic updates.
89551	Fixed an issue where User Activity Reports delivered via the Email Scheduler did not include usernames that contained German characters.
88646	Fixed an issue where predicted FTP sessions were not established as expected from the parent FTP session.
88346	Fixed an issue where a firewall was sending BGP packets with the wrong MD5 authentication value.
88327	Fixed an issue where several valid country codes were missing in the Certificate Attributes section when generating a certificate from the web interface.
88157	Fixed an issue with reduced throughput for traffic originating on the firewall and traversing a VPN tunnel.
87851	Fixed an issue where high rates of fragmented packets caused the firewall to experience a spike in packet buffer, descriptor, and CPU usage.
87741	Fixed an issue on PA-3000 Series firewalls where the dataplane restarted after an upgrade.
87179	Fixed an issue where a virtual system (vsys) in a Panorama template was assigned duplicate vsys numbers during commit to the firewall.
PAN-52038 86767	A security-related fix was made to address CVE-2015-7547 (PAN-SA-2016-0029).
86623	Fixed an issue where a firewall in an HA active/passive configuration dropped FTP PORT command packets after a failover.
86123	Fixed an issue where an M-100 appliance in an HA pair had a process (*configd*) repeatedly restart, causing HA sync to fail.
85160	Fixed an issue where a firewall lost members of a domain group after a failover from the primary to the secondary LDAP server when the last modified timestamp for the group was not the same on both servers.

Issue ID	Description
84115	Fixed an issue where virtual system administrators (full access or read-only) were unable to access settings under the **Network** tab (`Panel for undefined not registered` was displayed, instead).
83239	Fixed an issue where inbound SSL decryption did not work as expected when you enabled SYN cookies.
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).
80953	Fixed an issue on firewalls in an HA active/active configuration that included virtual wire interfaces where packets did not adhere to virtual wire forwarding paths and caused MAC address flapping on neighbor.
77822	Fixed an issue on a VM-Series NSX edition firewall that sent Dynamic Address Group information only to the primary virtual system (VSYS1) on the integrated physical firewall at the data center perimeter. With this fix, a VM-Series NSX edition firewall configured to Notify Device Group sends Dynamic Address Group updates to all virtual systems on a physical firewall running PAN-OS 7.0.8 or a later PAN-OS 7.0 release.

PAN-OS 7.0.7 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.7 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

⚠ Before you upgrade to PAN-OS 7.0.3 or a later PAN-OS 7.0 release, review the information about how to upgrade a firewall to PAN-OS 7.0. Additionally, if virtual system (vsys) configuration is not enabled on your firewall or appliance, you must reboot your firewall or appliance after you install PAN-OS 7.0.1 and before you upgrade to PAN-OS 7.0.3 or a later release.

Issue ID	Description
94912	Fixed an issue in PAN-OS 7.0.6 where WF-500 appliances returned false positive results—primarily for Microsoft Word (.docx) files.
93775	Fixed an issue where packet diagnostics failed due to an unnecessarily large debug log related to HA3 packet forwarding.
93644	Fixed an issue on PA-3000 Series firewalls where processing jumbo frames that were larger than 7,000 bytes during a period of heavy traffic caused the FPGA to stop responding. With this fix, the FPGA thresholds are adjusted to correctly handle up to 9KB jumbo frames.
93612	A security-related fix was made to address a privilege escalation issue (PAN-SA-2016-0015).
93228	Fixed an issue on PA-7050 firewalls in an HA active/active configuration where jumbo frames that included the DF (do not fragment) bit were dropped when crossing dedicated HA3 ports.
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).
91771	Fixed an issue where a firewall did not send TCP packets out during the transmit stage in the same order as those packets were received.
91443	Fixed an issue where a Panorama M-100 appliance purged logs due to an incorrect quota size.
91079	Fixed an issue on a VM-Series firewall where an ungraceful reboot caused Dynamic IP address information to get out of sync.
91075	Fixed an issue where the LSVPN tunnel interface failed to pass traffic after upgrading a GlobalProtect LSVPN satellite to a PAN-OS 7.0 release while the GlobalProtect LSVPN gateway was still running a PAN-OS 6.1 or earlier release. Additionally, the tunnel interface flapped if you enabled tunnel monitoring. These issues occurred due to changes to the encryption algorithm names when introducing Suite B ciphers in PAN-OS 7.0. With this fix, GlobalProtect LSVPN satellites running PAN-OS 7.0.7 (or PAN-OS 7.1) or later releases successfully recognize the old names used in PAN-OS 6.1 and earlier releases so that LSVPN tunnels are established and pass traffic as expected.

Issue ID	Description
90433	Fixed an issue where overrides of the default rules in the Shared policy took precedence over the overrides of default rules in a device group. With this fix, override precedence now behaves as designed (overrides of default rules in the lowest level device group take precedence over those settings in the higher level device groups and Shared).
90194	Fixed an issue where firewalls without any WildFire public signatures (had never downloaded any or old signatures had been deleted) did not properly leverage WildFire private cloud signatures when monitoring traffic.
90158	Fixed an issue on PA-7000 Series firewalls where aggregate outbound traffic was incorrectly limited by the chassis switch fabric switching capacity.
90070	Fixed an issue where a memory leak associated with the authentication process (*authd*) caused intermittent access and authentication issues.
90029	Fixed an issue where a GlobalProtect gateway rejected the same routes learned from different LSVPN satellites when the routes were destined for a different virtual router.
89761	Fixed an issue where a scheduled log export failed to export the logs if the password in the configuration contained the dollar sign ($) character.
89588	Fixed an issue where packets that had to be retransmitted during SSL decryption were not handled correctly, which resulted in a depleted software packet buffer.
89503	Fixed an issue where user-group mappings were not properly populated into the dataplane after a firewall reboot.
89413	Fixed an issue where Panorama template commits failed when the names of several certificates in the Default Trusted Certificate Authorities list changed. This occurred when Panorama was running a PAN-OS 7.0 release and pushed a template to a firewall running a PAN-OS 6.1 or earlier release.
89385	Fixed an issue with firewalls in an HA active/active configuration where session timeouts for some traffic were unexpectedly refreshed after a commit or HA sync attempt. ⚠ This fix introduced a known issue: PAN-59037 (97806).
89296	Fixed an issue where a commit failed after renaming a Panorama shared object that was already referenced in the rules on a local firewall.
89108	Fixed an issue where a firewall did not advertise prefixes to some BGP peers when expected.
88689	Fixed an issue where a memory leak associated with the authentication process (*authd*) caused commit attempts to fail.
88450	Fixed an issue where Layer 3 interfaces without defined IP addresses, zones, or virtual routers dropped LLDP packets, which prevented the firewall from obtaining and displaying neighbor information.
88421	Fixed an issue where WildFire reports were generated for files already blocked by the Antivirus profile SMTP decoder.
88325	Fixed an issue where a PA-500 firewall running a PAN-OS 7.0.1 or later release and with DNS Proxy enabled failed to connect to User-ID agents using FQDN.

Issue ID	Description
88313	Fixed an issue where read-only device administrators were unable to view logs on the **ACC** tab.
87911	Fixed an issue where scheduled dynamic updates to managed firewalls stopped functioning after migrating the Panorama VM to an M-500 appliance.
87880	Fixed an issue where the XML API request to test Security policy was not properly targeted to a specified virtual system (vsys), which made the request applicable only to the default vsys. With this fix, the XML API request to test Security policy is able to retrieve results for any previously targeted vsys.
87833	Fixed an issue where WildFire updates caused the interface to flap.
87729	Fixed an issue where the dataplane on the passive firewall in a synced HA configuration restarted due to a Decryption profile that didn't have any associated Decryption policy rules, which resulted in SSL proxy sessions that were dropped on the passive firewall when the active firewall became suspended during a failover.
87594	Fixed an issue on M-Series appliances that caused the `show ntp` CLI command to time out.
87094	Fixed an issue where committing a policy on Panorama that contained interfaces that were manually defined generated the error: `[interface name] is not an allowed keyword.`
86977	Fixed an issue where LDAP sessions sourced from Panorama, a firewall, or an M-100 appliance were kept open and not actively refreshed, which caused sessions to timeout when they traversed the peer firewall (or the dataplane on the same firewall) and, ultimately, caused authentication attempts to fail when requests could no longer reach the LDAP server. With this fix, a keep-alive mechanism is added that is triggered after 15 minutes of session inactivity and that allows a maximum of five failed probes before dropping a connection (probes occur in 60-second intervals).
86821	Fixed an issue where the server process (*devsrvr*) stopped responding when attempting to access a URL with multiple nested children, which caused the dataplane to restart.
86686	Security-related fixes were made to address issues reported in the October 2015 NTP-4.2.8p4 Security Vulnerability Announcement.
86313	Fixed an issue where the `failed to handle CONFIG_COMMIT` error was displayed during a commit.
86202	Fixed an issue where the management plane stopped responding if you modified an object referenced in a large number of rules.
86189	Fixed an issue where the firewall did not send SNMPv3 traps that used an IPv6 server address.
86122	Fixed an issue where an LACP Aggregate Ethernet (AE) interface using SFP copper ports remained down after a dataplane restart.
85344	Fixed an issue where scheduled dynamic update installation caused the HA link to flap.
85265	Fixed an issue in the XML API that prevented a read-only superuser from downloading custom packet captures.
84997	Fixed an issue on PA-7000 Series firewalls where the first autocommit attempt failed.

Issue ID	Description
84461	Fixed a Panorama issue where the virtual memory for a process (*configd*) exceeded its allocation, which caused commit and HA sync attempts to fail.
84146	Fixed an issue in PAN-OS 7.0 releases where the source and destination field was no longer included as expected in error messages that were triggered when requests to delete address objects failed. With this fix, the source and destination information is again included in the error message.
84027	Fixed an issue where a firewall allowed some HTTP GET packets to pass through even when the URL Filtering profile was configured to block packets in this URL category.
83564	Fixed an issue where a certificate Common Name (CN) containing UTF-8 characters caused commit requests to fail because the decoded CN string exceeded the 64-character limit.
82918	Fixed an issue where re-entering an LDAP bind password through the CLI using a hash value (instead of a regular password) was rejected for having too many characters.
77460	Fixed an issue on a firewall with an expired BrightCloud license where the specified vendor was unexpectedly and automatically changed from BrightCloud to PAN-DB when any feature auth code was pushed from Panorama to the firewall.
76661	Fixed an issue where voltage alarms were triggered incorrectly (voltage was within the appropriate range).
74443	A security-related fix was made to address CVE-2015-0235.
73082	Fixed an issue where a firewall process (*all_pktproc*) stopped responding due to an issue with NAT pool allocation.

PAN-OS 7.0.6 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.6 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Before you upgrade to PAN-OS 7.0.3 or a later PAN-OS 7.0 release, review the information about how to upgrade a firewall to PAN-OS 7.0. Additionally, if virtual system (vsys) configuration is not enabled on your firewall or appliance, you must reboot your firewall or appliance after you install PAN-OS 7.0.1 and before you upgrade to PAN-OS 7.0.3 or a later release.

For WF-500 appliances, the PAN-OS 7.0.7 maintenance release addresses an issue that was introduced in PAN-OS 7.0.6 that causes frequent false positive verdicts for Microsoft Office documents. You are advised to upgrade WF-500 appliances to 7.0.7 or later releases and are advised not to install the 7.0.6 image.

Issue ID	Description
92671	Fixed an issue where traffic that was offloaded to hardware was not forwarded properly. This occurred on PA-3050 and PA-3060 firewalls and primarily with SSL traffic.
90992	Fixed an intermittent issue where the initial GlobalProtect client connection to a GlobalProtect portal or gateway failed with the error: `Valid client certificate is required`. This occurred when the certificate profile used CRL/OCSP to check certificate validity and was due to a problem with the certificate not being available in the dataplane cache. Subsequent connections worked because the certificate was added to the cache during the initial connection attempt.
90904	Fixed a packet drop issue on PA-7000 Series firewalls in HA configurations running a PAN-OS 7.0.3 through PAN-OS 7.0.5 release. This occurred due to a MAC address lookup issue on interfaces in an Aggregate Ethernet (AE) interface group that were part of a VLAN.
89881	Fixed an issue where the User-ID™ agent truncated NetBIOS names with more than 14 characters. As a result, users with domain names longer than 14 characters were not granted access.
89880	Added a new CLI operational command (`set authentication radius-auth-type <auto|chap|pap>`) for M-Series appliances in Panorama™ mode to address an incompatibility issue between PAN-OS and some RADIUS servers. With this fix, you can manually override the automatic selection mechanism and choose between CHAP and PAP.
89317	Fixed an issue where improper data pattern ordering occurred after an administrator deleted data patterns from an existing Data Filtering profile, which subsequently caused an error (`rule is already in use`) when attempting to add a new data pattern. With this fix, you can add or delete data patterns in any order.
88794	Fixed an issue where one-time password (OTP) RADIUS authentication failed when the domain selection field was used in the authentication profile.
88696	Fixed an issue where, under certain conditions, a process (*mpreplay*) frequently restarted due to excessive internal messaging.

Issue ID	Description
88570	Fixed an issue where a Neighbor Solicitation (NS) packet—used to refresh IPv6 neighbor tables—was sent out through a VLAN interface without a VLAN tag. The NS packet was tagged correctly when the neighbor entry was initially created but the packet used to refresh the table was sent without the tag, which caused the table update to fail when the neighbor did not receive an appropriately tagged response.
88168	Fixed an issue where VM-Series firewalls running on an 8-core platform changed the passive firewall to active when a socket error occurred. The socket remained closed until an interface-related change was made.
88125	Fixed an issue where TCP segments for DNS queries were dropped when the segments were smaller than 12 bytes.
87482	A security-related change was made to management plane account restrictions to avoid service disruption.
87285	Fixed an issue where a User Activity Report PDF for the last 30 days generated an error when the report contained more than 100,000 lines.
87257	Fixed an issue that caused a dataplane restart when the firewall was configured as a DHCP relay and received DHCP requests from a third-party DHCP server or client that exceeded the payload length specified in RFC-2132.
87158	Fixed an issue where some packets were duplicated in the egress stage. This occurred on multi-dataplane firewalls when traffic flowed from virtual system to virtual system or from virtual system to a shared gateway. An update has been made to prevent packet duplication.
86980	Fixed an intermittent issue where commits failed due to invalid file permission warnings related to SSH authentication.
86970	Fixed an issue where decryption on the firewall did not function when using Chrome to browse certain websites because Chrome eliminated insecure fallback to TLS 1.0.
86916	Fixed an issue where traffic bursts entering a PA-3000 Series firewall caused short-term packet loss even though the overall dataplane utilization remained low. This issue was typically observed when two firewall interfaces on the same firewall were connected to each other. With this fix, internal thresholds were modified to prevent packet loss in these conditions.
86671	Fixed an issue where Panorama did not recognize threat IDs generated by a WF-500 appliance, which prevented you from configuring an exemption for these threats in Panorama that could be pushed to managed firewalls.
86633	Fixed an issue where the web interface indicated that a new DHCP relay configured in the CLI was enabled even though the relay was not, yet, enabled from the CLI.
86321	Fixed an issue where SSH decryption caused a dataplane memory leak and restart.
86251	Fixed an issue where an administrator was unable to retrieve log partition utilization using SNMP after adding additional virtual disk space on Panorama.
85913	Fixed an issue where an administrator was unable to add more than one X-Auth GlobalProtect gateway on the same interface.
85880	Enhanced the syslog variable list to include `cef-number-of-severity`.

Issue ID	Description
85110	Fixed an issue where the firewall sent gratuitous ARP (GARP) packets for an interface IP address used in a destination NAT rule from all interfaces in the zone where that interface belonged. With this fix, the GARP packets are sent only from the interface that owns the IP address.
84949	Fixed an issue where M-100 appliances in an HA active/active configuration forwarded logs only to one syslog server, even though two syslog servers were defined. This issue occurred only on the primary-secondary appliance and was due to an HA sync issue.
84665	Fixed an issue where the **Commit** icon incorrectly indicated pending configuration changes after an Applications and Threats update.
84641	Fixed an issue where some DNS requests were forwarded to the wrong DNS server—the one previously but no longer configured on the firewall.
84339	Fixed an issue where a single session consumed the majority of the packet buffer resources. With this fix, you can use information in the output of the `show running resource-monitor ingress-backlogs` command to Identify Sessions That Use an Excessive Percentage of the Packet Buffer and then use the `request session-discard` CLI operational command to manually discard sessions as needed. These commands are only available on firewalls that support hardware offload.
84236	Fixed an issue where special characters in the SNMPv3 **Users** field caused encryption to fail and caused the firewall to restart.
83722	Fixed an issue where destination-based service routes did not work for RADIUS authentication servers.
83702	Fixed an issue on PA-7000 Series firewalls running PAN-OS 7.0.2 and later releases where WildFire™ Analysis reports did not display in the **WildFire Analysis Report** tab (**Monitor > Logs > WildFire Submissions > Detailed Log View**).
83361	Fixed an issue where the DoS classification counter stopped at an abnormally high value. This caused flood type false positives in the Threat logs, causing the firewall to appear as if it reached maximum session capacity.
83135	Fixed an issue where the initial redirect failed for some SSL sites. (The error—`Bad Record MAC`—appeared after the user clicked continue but the user could then refresh the page to successfully enter the website.)
83100	Fixed an issue where Panorama HA synchronization failed when attempting to upgrade to a PAN-OS 7.0.1 through PAN-OS 7.0.5-h2 release.
82756	Fixed an issue where custom reports were not sent out by the Email Scheduler.
82443	Fixed an issue where unwanted characters were displayed on the login page after a failed login.
80721	Fixed an issue where the XML API command `show dos-protection rule statistics` (used to retrieve DoS protection statistics) returned an error: `invalid command option`.
80507	Fixed an issue in Panorama where Threat and Content names for certain threats did not appear in ACC reports, predefined reports, and spyware reports. This issue occurred only on PA-7000 Series firewalls managed by Panorama and only during an Antivirus update.

Issue ID	Description
79729	Fixed an issue with firewalls in an HA configuration where a commit operation aborted for all daemons and then the DHCP daemon stopped responding. This occurred when the `set deviceconfig high-availability group {group-name} configuration-synchronization enabled` option was set to `no`.
78090	Fixed an issue where the User-ID process stopped responding on both peers in an HA active/passive configuration. This issue occurred after an upgrade and was due to a problem with the LDAP library.
74333	Fixed an issue where incremental updates for new and updated registered IP addresses were failing when registration events were occurring through the XML API. With this fix, integrating the updates for registered IP addresses no longer fails when using the XML API (on either standalone firewalls and appliances or those in HA configurations).

PAN-OS 7.0.5-h2 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.5-h2 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Before you upgrade to PAN-OS 7.0.3 or a later PAN-OS 7.0 release, review the information about how to upgrade a firewall to PAN-OS 7.0. Additionally, if virtual system (vsys) configuration is not enabled on your firewall or appliance, you must reboot your firewall or appliance after you install PAN-OS 7.0.1 and before you upgrade to PAN-OS 7.0.3 or a later release.

Issue ID	Description
89750	A security-related fix was made to address a stack underflow condition.
89706	A security-related fix was made to prevent some CLI commands from improperly executing code.

PAN-OS 7.0.5 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.5 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

> Before you upgrade to PAN-OS 7.0.3 or a later PAN-OS 7.0 release, review the information about how to upgrade a firewall to PAN-OS 7.0. Additionally, if virtual system (vsys) configuration is not enabled on your firewall or appliance, you must reboot your firewall or appliance after you install PAN-OS 7.0.1 and before you upgrade to PAN-OS 7.0.3 or a later release.

Issue ID	Description
89752	A security-related fix was made to address a buffer overflow condition.
89717	A security-related fix was made to ensure the appropriate response to special requests received through the API interface.
88550	Fixed an issue on firewalls running in Common Criteria (CC) mode where seeding using an OpenSSL deterministic random bit generator (DRBG) caused a process (*cryptod*) to stop responding and resulted in commit failures.
88439	Fixed an issue on a PA-3000 Series firewall where a dataplane constantly restarted due to a hardware content matching memory issue.
88382	Fixed an issue in a high availability (HA) active/active configuration with unexpectedly short (20 second) timeouts that occurred when an HA2 session sync message failed. This issue was due to an ARP problem between dataplanes in the HA configuration when the HA2-backup was in use and using either IP or UDP transport mode. With this fix, unexpectedly short session timeouts no longer occur due to this issue.
88191	A security-related fix was made to address information leakage in systems log that impacted the web interface (PAN-SA-2016-0016).
87565	Fixed an issue where a firewall did not forward correlation events to the syslog server.
87170	Fixed an issue where a firewall did not filter groups using the filters applied in search parameters; instead, the firewall ignored filters and displayed all groups in search results.
86947	Fixed a rare issue where an active firewall in a high availability (HA) configuration incorrectly synced to the configuration from the passive firewall when a second commit was performed on the active firewall before a previous commit was completed.
86723	Fixed an issue where a dataplane restarted when client-to-server traffic exceeded 4GB and included HTTP GET or POST requests that had the source IP address in the Origin header.
86664	Fixed an issue with IKEv2 that caused a child security association (SA) to install incorrectly on a firewall when the tunnel was connected to third-party equipment using PFS.
86390	Fixed an issue where a virtual system (vsys) created in a Panorama template did not display where expected when the first two characters of the vsys name was "sg" (such as "sg01"). With this fix, Panorama no longer allows you to create a vsys with a name that begins with "sg" in a Panorama template.

Issue ID	Description
86319	Fixed an issue where a process (*routed*) on the firewall stopped responding and resulted in high CPU usage when applying a BGP autonomous system (AS) path filter.
86312	Fixed an issue where the `last update` time never exceeded 1 second after making a change to the update interval of a group mapping service.
86193	Fixed an issue in a high availability (HA) configuration where LDAP group mappings did not properly refresh after a firewall became the active peer again after going through the passive state. This was due to a variable that was not initialized properly and was then used in an error case. With this fix, LDAP variables are properly initialized to avoid this LDAP group mapping issue.
86136	Fixed an issue where the GlobalProtect gateway sent an access-request packet with malformed data inside the Framed-IP-Address field to the RADIUS server.
86126	Fixed an issue where a user with a custom role-based administrative account couldn't preview rules listed as Combined rules.
86091	Fixed an issue where a commit to configure a tunnel interface that used a string instead of an integer caused a process (*routed*) on the firewall to stop responding.
86075	Fixed an issue on a PA-3060 firewall where the size of the *SML VM EmlInfo* software pool was less than expected. With this fix, the size of the SML VM EmlInfo software pool is increased to the expected value.
85888	Fixed an issue where Panorama ignored the session timeout value and automatically refreshed administrators who were still logged in to the Panorama appliance even when those sessions were inactive for a period longer than the configured timeout.
85879	Fixed an issue where a firewall in a high availability (HA) configuration generated a false positive event (`Running configuration not synchronized after retries`) 75 seconds after each HA sync. With this fix, this error is returned only for commits that take longer than 45 minutes to complete.
85878	In response to an issue where DNS queries sometimes caused a Log Collector to run too slowly and caused delays in log processing, the `debug management-server report-namelookup disable` CLI command is added to disable DNS lookups for reporting purposes.
85863	Fixed an issue where multicast traffic sent over a virtual wire (vwire) with **Multicast Firewalling** disabled (**Network > Virtual Wires > <*vwire*>**) caused high CPU and packet buffer depletion.
85821	Fixed an issue where a dataplane stopped responding due to memory corruption.
85754	Fixed an issue where a VM-Series disk was corrupted and went into maintenance mode after processing mutated traffic from third-party signature detection software.
85687	Fixed an issue where the system log entries displayed `logged in via Web from 127.0.0.1` for administrators who logged in via XML API. With this fix, the system log displays the correct IP address for administrators who logged in via XML API.
85675	Fixed an intermittent issue where a process (*mprelay*) restarted and, after multiple restarts, caused the firewall to restart. This issue was associated with the processing of add and delete events for IPv4 ARP and IPv6 neighbor updates. With this fix, IPv4 ARP and IPv6 neighbor updates no longer cause the mprelay process or firewall to restart.

Issue ID	Description
85611	Fixed an issue where the `number of fib entries for device` FIB counter was inaccurate with ECMP enabled. With this fix, the firewall maintains an accurate count of entries in the FIB table for the `number of fib entries for device` FIB counter.
85484	Fixed an intermittent issue where the GlobalProtect portal used the cookie instead of the authentication information provided by the GlobalProtect client, which caused authentication to fail. With this fix, if a client connects using a cookie, the GlobalProtect portal ignores the cookie in favor of the authentication information provided by the GlobalProtect client so that authentication is successful.
85358	Fixed an issue where SSL decryption sessions were not cleared after executing the `clear session all filter ssl-decrypt yes` CLI command (or any other session clearing command that used the `ssl-decrypt yes` filter). With this fix, SSL decrypt sessions are cleared as expected when executing session clearing commands that include the `ssl-decrypt yes` filter.
85245	Fixed an issue where a virtual system (vsys) configuration remained in the firewall configuration even after the vsys was deleted. This caused commits to fail when attempting to add a new vsys using the same ID as the vsys that was not successfully deleted.
85193	Fixed an issue in a high availability (HA) configuration where multiple overlapping queries resulted in a race condition that caused HA sync jobs to fail.
84963	Fixed an issue in Panorama templates where administrators could mark a certificate as Forward Trust or Forward Untrust but forwarding did not take place as expected when the template was configured to apply only to one virtual system (single vsys mode). With this fix, marking a certificate as Forward Trust or Forward Untrust works as expected even when the template is in single vsys mode.
84908	Fixed an issue where the logged session end reason for decrypted SSL sessions always displayed as `aged out` regardless whether that was the actual TCP session end reason. With this fix, the session end reason now displays correctly for decrypted SSL sessions.
84729	Fixed an issue on M-Series appliances and with PA-7000 Series Log Processing cards where output of the `show system logdb-quota` CLI command didn't match the values in Logging and Reporting Settings in the web interface (**Device > Setup > Management > Logging and Reporting Settings > Log (Card) Storage**) due to a discrepancy in space calculation. With this fix, the values in the web interface accurately reflect available storage space and match the output from the `show system logdb-quota` CLI command.
84552	Fixed an issue where the `debug user-id reset ts-agent/user-id-agent` CLI command did not work as expected.
84538	Fixed an issue where a dataplane restarted unexpectedly on a firewall with SSL decryption enabled. This occurred during the SSL handshake when the firewall received a Hello packet from the server that had a higher SSL protocol version than the Hello packet received from the client.
84496	Fixed an issue on PA-7000 Series firewalls where excessive or prolonged log queries caused a memory leak on the Log Processing Card (LPC).
84239	Fixed an issue where a read-only Superuser was able to perform a commit when using XML API (but not via the web interface). With this fix, read-only Superusers cannot use XML API to perform commits.
83764	Fixed an issue where using web interface certificate authentication caused login failures.

Issue ID	Description
83731	Fixed an issue in a virtual wire configuration where a firewall incorrectly modified the MAC address for traffic when decryption was enabled. With this fix, the firewall no longer modifies the MAC address of traffic.
83454	Fixed an issue with IPv6 traffic that had an extension header and caused jitter when passing through a PA-7000 Series firewall in a high availability (HA) active/active configuration.
83362	Fixed an issue where a commit failed when a subinterface that was pushed from Panorama lost its reference to its associated VLAN after the subinterface configuration on the firewall was overridden and then reverted in the template. With this fix, after an interface is reverted, subinterfaces do not lose their mapping to VLANs.
83337	Fixed an issue where firewalls generated multiple core dumps after a reboot when incoming packets were forwarded to the dataplane while an autocommit was still processing. With this fix, packets are not forwarded to the dataplane until an in-process autocommit is complete.
83145	Fixed an issue on a PA-7000 Series firewall where an interface in tap mode unexpectedly transmitted traffic that was received on that interface.
82916	Fixed an issue where the trusted CA store on the firewall was missing the QuoVadis root CA2 and root CA3 G3 certificates. With this fix, both these QuoVadis certificates are included in the trusted CA list.
82873	Fixed an issue with missing fields and inconsistencies in the Syslog format for Correlated Events that were exported to a syslog server.
82862	Fixed an issue where the device server process (*devsrvr*) restarted unexpectedly when Panorama pushed a template that contained a certificate with a corrupt public key.
82667	Fixed an issue where the PAN-OS integrated User-ID agent failed to connect to a monitored server when the User-ID agent was configured to use the FQDN instead of the IP address for the server.
82358	Fixed an issue where, when using LDAP authentication, a GlobalProtect client incorrectly showed a `Password expired` message even when the password had not expired.
81812	Fixed an issue where a firewall did not accurately check certificate revocation status via OCSP because the OCSP request did not include the HOST header option. With this fix, the firewall uses the HOST header option as expected and successfully retrieves the revocation status of the certificate in response to OCSP requests.
81743	Fixed an issue where URL categorization failed for some URLs due to an issue with message buffer size.
81425	Fixed an issue where IPSec renegotiation was not initiated as expected after a PPPoE interface received a new IP address.
81424	Fixed an issue where the `From` column in the output of the `show admins` command was `Console` instead of the correct IP address when connected to the CLI via telnet or SSH.
81062	Fixed an issue where the email action for scheduled reports timed out due to reports that took too long to generate. With this fix, the email timeout is increased and report generation is enhanced to avoid this issue.

Issue ID	Description
80415	Fixed an issue where a firewall was not presenting the Captive Portal response page to users. This occurred when the URL category was marked `not-resolved`, such as when cloud servers were unavailable.
79596	Fixed an intermittent issue on PA-5000 Series firewalls where the dataplane stopped responding. With this fix, there are additional sanity checks and logging to avoid this issue.
73177	Fixed an issue where redistributed Not-So-Stubby Area (NSSA) type 7 routes converted to NSSA type 5 routes were not flushed from the OSPF database quickly enough after the redistributing NSSA router went down. With this fix, the OSPF is flushed within the expected period of time so that routes that go down are not advertised as still available.

PAN-OS 7.0.4 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.4 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

> ⚠ Before you upgrade to PAN-OS 7.0.3 or a later PAN-OS 7.0 release, review the information about how to upgrade a firewall to PAN-OS 7.0. Additionally, if virtual system (vsys) configuration is not enabled on your firewall or appliance, you must reboot your firewall or appliance after you install PAN-OS 7.0.1 and before you upgrade to PAN-OS 7.0.3 or a later release.

Issue ID	Description
88869	Fixed a performance degradation issue on a VM-Series firewall with 8 cores when threat scanning was enabled when attempting to process large transaction-specific SSL traffic types. Additionally, this fix addressed an intermittent issue where the GlobalProtect MSI file failed to download after a user authenticated to the portal page.
87422	Fixed an issue where multicast traffic was dropped when the source started sending group traffic because there was not, yet, a corresponding multicast route or FIB entry on the firewall. With this fix, the multicast route is updated more quickly and packets are enqueued instead of dropped while the firewall waits for the updated route information.
87410	Fixed an issue where an API call to add, delete, or modify a URL entry failed when the URL included a single (') or double (") quote character as an XML attribute. With this fix to comply with XML Xpath 1.0, API instructions are completed successfully even when acting on a URL that includes a single or double quote used as an XML attribute.
87385	Fixed an issue where all the widgets on the **ACC** tab of a managed firewall (and when exported in a PDF file) display `Report Error` when you access the firewall through a context switch from Panorama (whether virtual or M-Series appliance).
87280	Fixed an issue where the number of SSL free memory chunks was depleted to 0, which caused a disruption in SSL decryption-related traffic.
87231	Fixed an issue where a PA-7000 Series firewall did not load-balance egress traffic on Aggregate Ethernet (AE) interfaces as expected.
87078	Fixed an issue where the management server stopped responding where there was a high logging rate, which caused the Log Collector to disconnect from Panorama.
86938	The client certificate used by PAN-OS and Panorama to authenticate to the PAN-DB cloud service, the WildFire cloud service, and to WF-500 appliances 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 7.0 release to PAN-OS (or Panorama) 7.0.4 or a later release.
86895	Fixed an issue on M-Series and WF-500 appliances where the Ethernet1/2 interface unexpectedly broadcasted DHCP discover packets with the internal BMC IPMI LAN MAC address as the source MAC address when the internal BMC IPMI LAN was configured to use DHCP as the source address.

Issue ID	Description
86803	Fixed an intermittent issue where the idle timer for GlobalProtect IPSec tunnels either did not expire appropriately (such as when the tunnel was torn down) or expired at the configured idle time expiration even when a user was actively using the connection. With this fix, the GlobalProtect IPSec tunnel idle timer behaves as expected.
86467	Fixed an issue in PAN-OS 7.0.3 where firewalls did not check for superuser accounts that were pushed through a Panorama template, which caused an upgrade process error when all superuser accounts were pushed through a Panorama template (firewalls must have at least one superuser account in the configuration). With this fix, firewalls correctly recognize superuser accounts that are pushed through a Panorama template.
86212	Added a new CLI operational command (`set authentication radius-auth-type <auto|chap|pap>`) to address an incompatibility issue between PAN-OS and some RADIUS servers. With this fix, you can manually override the automatic selection mechanism introduced with Challenge-Handshake Authentication Protocol (CHAP) support in PAN-OS 7.0 to select either CHAP or Password Authentication Protocol (PAP) as needed.
85801	Fixed an issue where a firewall that was forwarding logs to multiple Panorama management servers and Log Collectors stopped forwarding logs to any appliance after an administrator suspended log forwarding on the active primary Panorama server. With this fix, the firewall continues to forward logs to all Panorama management servers and Log Collectors except any appliance for which an administrator specifically suspends log forwarding.
85721	Fixed an issue where firewalls with a specific OCZ Deneva hard disk (model DENCSTE251M21) configured in a RAID and running PAN-OS 7.0.1 or later releases experienced RAID errors.
85514	Fixed an issue where a commit request failed due to processes (*configd* and *mongod*) with high memory usage.
85364	Fixed an issue where HTTP and HTTP Online Certificate Status Protocol (OCSP) management services were enabled only for the first IP address on an interface with multiple IP addresses. With this fix, when HTTP and HTTP OCSP management services are enabled on an interface, services are enabled for all IP addresses associated with that interface.
85285	Fixed an issue where output from the `show ntp` command did not always display the correct NTP status. Primarily, this issue occurred when there was only one NTP server configured and, even when correctly connected to the NTP server, the output of the `show ntp status` command displayed as `rejected`. With this fix, output from the `show ntp` command correctly displays NTP status as `synchronized` after the firewall successfully connects to an NTP server.
85166	Fixed an issue on a PA-7000 Series firewall where the first packet in a session was dropped when it arrived before the firewall freed up a previous session that used the same 5-tuple. With this fix, the firewall treats the previous session as an inactive flow and successfully creates the new session.
85091	Fixed an issue on a firewall where software packet buffers were being depleted. With this fix, the firewall will dynamically adjust the TCP receive window based on peer traffic to avoid software packet buffer depletion. Additionally, there is a fix for a memory leak in error handling of SSL Forward Proxy mode and the size of the software buffer pools is increased.

Issue ID	Description
84851	Fixed an issue where the virtual system (vsys) ID on the firewall was computed incorrectly when Panorama pushed a template with **Force template value** enabled and containing virtual system information to the firewall.
84811	Fixed an issue on a VM-Series firewall (KVM on Centos7/Redhat) where a process (*vm-uuid*) displayed as empty after boot. With this fix, the vm-uuid process is displayed correctly.
84678	Fixed an issue with the way the management plane performed updates through HTTP and HTTPS calls, such as for block list and content updates.
84595	Fixed an issue with HTTP requests generated by the firewall when retrieving custom Dynamic Block Lists.
84495	Fixed an issue where, in some cases, generating output for the `show running url-cache all` CLI command caused a short delay in communication with the dataplane. With this fix, to avoid this communication delay, the output of the `show running url-cache all` command is no longer included when generating the tech support file.
84494	Fixed an issue where the session end reason for a single threat ID was reported differently depending on which decoder was used. With this fix, only one session end reason (threat) is reported for all blocked SMTP traffic regardless which decoder is used.
84465	Fixed an issue where the external interface on an LSVPN satellite was unable to establish an LSVPN connection to the active-primary firewall in an HA active/active configuration that was acting as the GlobalProtect portal or gateway when the external interface of the satellite was configured as a DHCP client. (This failure occurred even though an LSVPN connection was successfully established with the active-secondary firewall.) With this fix, the LSVPN satellite (with the external interface configured as a DHCP client) successfully establishes an LSVPN connection to both firewalls (active-primary and active-secondary) after a reboot.
84454	Fixed an issue where attempts to load a partial configuration for a device group from an XML file resulted in an error message. With this fix, you can successfully load a partial configuration for a device group and merge it with an existing device group.
84433	Fixed an issue where a web page would not load successfully without refreshing the browser multiple times when Open Certificate Status Protocol (OCSP) validation was enabled. This occurred when a block page message was presented within one second of the attempt to load an HTTPS site while decryption was enabled on the firewall with the OCSP validation timeout set to 60 seconds.
84167	Fixed an issue where a firewall incorrectly reordered certain TCP traffic during transmit stage.
84008	Fixed an issue where an LSVPN IPSec tunnel went down when the hard key lifetime expired during a re-key. With this fix, the soft key lifetime is adjusted so that the hard key lifetime does not expire before the re-key finishes.
83907	Fixed an issue where administrators could not disable counters in system logs using the `debug dataplane packet-diag set log counter <counter-name>` CLI command when those counters had names longer than 31 characters.
83902	Fixed an issue where monitoring an SNMP OID (.1.3.6.1.2.1.25.2.3.1.5.41) for disk space resulted in incorrect values on volumes over 2TB in size.

Issue ID	Description
83898	Fixed an issue on Panorama M-Series and virtual appliances where exporting a report as a comma-separated value (CSV) file (**Monitor > Reports**) failed and resulted in a web interface error (`Error enqueuing export job`).
83889	Fixed an issue where a PA-7000 Series firewall incorrectly dropped non-TCP and non-UDP fragmented traffic, such as EtherIP traffic.
83844	Fixed an issue where a memory leak caused a PA-200 firewall to reboot.
83657	Fixed an issue where Panorama did not properly push device or template configurations for NTP, send-hostname-in-syslog, or WildFire settings to a device.
83592	Fixed an issue where the User-ID process (*useridd*) went into a reboot loop and caused the passive firewall in a high availability (HA) configuration to restart. This was due to bulk and incremental updates of terminal services users.
83253	Fixed an issue where video calls failed when H.245 (*openlogicalchannelack*) packets referenced a pre-NAT address.
82913	Fixed an issue where ToS headers were not set correctly in Encapsulating Security Payload (ESP) packets across VPN tunnels.
82865	Fixed an issue with a PA-5000 Series firewall where sessions owned by dataplane 1 (DP1) or DP2 did not display in the output when executing the `show session` command on DP0.
82710	Fixed an issue where unexpected dataplane restarts occurred due to out of memory errors and high resource usage on packet descriptors when SSL Forward Proxy was enabled. This fix also addresses a dataplane process memory leak.
82621	Fixed an intermittent issue on a PA-7000 Series firewall where traffic was dropped when the log interface and dataplane interfaces were both configured on the same Network Processing Card (NPC).
82605	Fixed an issue where policy-based forwarding (PBF) with **Enforce Symmetric Return** enabled (**Policies > Policy Based Forwarding >** *pbf-rule* **> Forwarding**) caused offloaded PBF sessions to fail when attempting to egress the firewall.
82424	Fixed an issue on a PA-5000 Series firewall where packets were dropped or the dataplane stopped responding when receiving specific ingress or egress traffic associated with offloaded sessions. With this fix, a field-programmable gate array (FPGA) change was made to address these issues.
82138	Fixed an issue where WildFire reports were not displayed on the web interface when proxy settings were configured for the management interface.
82118	Fixed an issue on the **QoS Statistics** panel (**Network > QoS**) where data was displayed only on the **bandwidth** tab; all other tabs (**Applications**, **Source Users**, **Destination Users**, **Security Rules**, and **QoS Rules**) were empty.
82095	Fixed an issue where a commit request did not finish processing due to a process (*routed*) that stopped responding.
81996	Fixed an issue where a HIP Profile did not sync between the active and passive firewalls in a high availability (HA) configuration, which caused the HIP Profile to no longer be in effect after a failover. With this fix, the HIP Profile is correctly synced between the active and passive firewalls and remains in effect after a failover.

Issue ID	Description
81949	Fixed an issue where Dynamic Address Groups pushed from Panorama to a firewall were not displayed in the output of CLI `show` commands.
81830	Fixed an issue where SSL Forward Proxy did not include the appropriate TLS 1.2 extension (Signature Algorithms) in Client Hello messages, which prevented successful interoperability with some Microsoft websites.
81333	Fixed an issue where managed firewalls and appliances were unable to connect to Panorama using the master key after a factory reset (or RMA).
81241	Fixed a rare issue where NAT traffic was dropped after a failed commit attempt.
80631	Fixed an issue in a high availability (HA) configuration where the ports on the passive firewall did not come up when the passive link state was set to **auto** (**Device > High Availability > General >** Active Passive Settings).
79917	Fixed an issue on a PA-3000 Series firewall where the dataplane stopped responding when receiving specific ingress or egress traffic associated with offloaded sessions. With this fix, a field-programmable gate array (FPGA) change was made to address this issue.
79531	Fixed an issue where an error was displayed (`No Data to Display`) in the Threat Monitor window (**Monitor > App Scope > Threat Monitor**) when selecting the **Show Files** filter.
78624	Fixed an issue where the active-secondary firewall in an HA active/active configuration was incorrectly responding to ARP requests for the IP address used in the destination NAT rule with binding to the active-primary firewall.
78482	Fixed an issue where VM Information Sources bypassed proxy settings.
78317	Fixed an issue where the management plane in an HA active/passive configuration restarted due to a dataplane process (*mprelay*) that stopped responding when it experienced memory corruption and encountered unexpected behavior from the FIB pointer.
77236	Fixed an issue where importing a certificate more than once with different names caused the dataplane to stop responding when the certificate was used for SSL Inbound inspection.
76269	Fixed an issue where an active-primary M-100 appliance in an HA configuration was unable to establish a connection with the passive-secondary or active-secondary HA peer for log collection.
76197	Fixed an issue where firewall Traffic logs displayed unusually large byte counts for `http-proxy` and `httpy-video` counters due to frequent application shifts between those application-type packets within a single proxy session.
76103	Fixed an issue where adding a threat exception to a Vulnerability Protection profile (**Objects > Security Profiles > Vulnerability Protection >** *profile* **> Exceptions**) resulted in an error (`Schema node for Xpath was not found`).
73187	Fixed an issue where the WildFire Analysis report (**Monitor > WildFire Submissions > Detailed Log View > WildFire Analysis Report**) did not display on versions 9 or 10 of Internet Explorer due to a script error.

Issue ID	Description
70719	In response to an issue where a dataplane restarted due to an incorrect flow ID, PAN-OS 6.1.4 and later releases included additional checks to help prevent the dataplane from restarting due to this issue. In PAN-OS 7.0.3, those PAN-OS 6.1.4 modifications were further modified to provide a more complete solution that avoids inadvertently dropping IPv4 traffic affected by this issue; in PAN-OS 7.0.4, the solution includes an additional fix to avoid inadvertently dropping IPv6 traffic related to this issue.
66285	Fixed an issue where the web interface certificate did not properly sync between HA peers, which led to a race condition that caused a commit request to fail.

PAN-OS 7.0.3 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.3 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

> Before you upgrade to PAN-OS 7.0.3 or a later PAN-OS 7.0 release, review the information about how to upgrade a firewall to PAN-OS 7.0. Additionally, if virtual system (vsys) configuration is not enabled on your firewall or appliance, you must reboot your firewall or appliance after you install PAN-OS 7.0.1 and before you upgrade to PAN-OS 7.0.3 or a later release.

Issue ID	Description
85065	Fixed a CLI input parsing issue that caused a process on the management plane to stop responding when processing unexpected input.
84711	Fixed an intermittent issue where some packets incorrectly matched Security policy rules, which resulted in App-ID™ policy lookup errors and discarding of packets.
84599	Fixed an issue in PAN-OS 7.0 releases where a process (*dhcpd*) did not correctly handle DHCP padding Option 0 when receiving DHCP request from the DHCP client. This prevented the firewall that was acting as the DHCP server from allocating and committing the offered IP address to the DHCP client, which caused the firewall to be stuck in offered state. With this fix, the DHCP process correctly handles DHCP padding Option 0 and successfully commits IP addresses offered to DHCP clients.
84246	Fixed an issue where a PA-7050 firewall running PAN-OS 7.0 assigned the same MAC address to all interfaces on two different PA-7050 chassis when the chassis base MAC addresses differed only in the 10th bit. With this fix in PAN-OS 7.0.3, two such different PA-7050 chassis are assigned different interface MAC addresses as expected.
84094	Fixed an issue where a user activity report (**Monitor > PDF Reports > User Activity Report**) contained no statistics for users with a domain+username string-length that exceeded 32 characters.
84046	Fixed an issue where SSL decryption failed when a certificate was rejected due to a missing or empty `basicConstraints` extension. With this fix, an exception is added to allow a missing or empty `basicConstraints` extension for self-signed non-CA certificates, and the following behaviors will be applied to CAs with regard to `basicConstraints` extensions: • If the CA has an extension `basicConstraints=CA:TRUE`, then allow the CA. • If the CA has an extension `basicConstraints=CA:FALSE`, then block the CA, but allow device-trusted CAs, including default CAs and imported CAs. • If the CA has does not have a `basicConstraints` extension, then block the CA, but allow device-trusted CAs, including default CAs and imported CAs, and allow self-signed CAs.
84012	Fixed an issue where a process (*ikemgr*) stopped responding due to a missing IKE profile.
83907	Fixed an issue where the `debug dataplane packet-diag set log counter <counter-name>` CLI command did not accept counter names longer than 31 characters, which prevented administrators from adding such counters for logging in system logs.

Issue ID	Description
83867	Fixed a rare issue where one of the internal databases was corrupted after an improper shutdown (power off) of the firewall. When this happened, the firewall was unable to automatically restart and would not startup properly thereafter.
83819	Fixed an issue on an M-100 appliance running Panorama™ 7.0 where a custom report failed to run when setting the Database (**Monitor > Manage Custom Reports**) to **Summary Databases > Remote Device Data > Threat** and selecting **Severity** from the list of Available Columns when any remote firewall used for custom reporting was running a PAN-OS 6.1 or earlier release.
83637	Fixed an issue where packet processing on a VM-Series firewall caused the firewall to stop forwarding traffic.
83574	Fixed a rare issue where, in some scenarios—such as when a firewall is restarted and IPSec security associations (SAs) are not established when a remote VPN peer is unreachable—the tunnel interface configured with IPSec tunnel monitoring is present in the routing table and status is `Up`.
83519	A security-related fix was made to address CVE-2015-5600.
83293	Fixed an issue in Panorama where SNMPv3 settings were removed and could not be updated when modifying an existing SNMPv3 device template.
83288	Fixed an issue where autocommit failed when the GlobalProtect gateway or Captive Portal certificate was pushed through Panorama after upgrading a firewall from a PAN-OS 6.1 release to PAN-OS 7.0.2.
83256	Fixed an issue where the firewall did not block unsupported elliptic curve Diffie-Hellman (ECDH) exchange cipher suites during SSL forward proxy even when **Block sessions with unsupported cipher suites** was enabled (**Objects > Decryption Profile >** *<decrypt-profile>* **> SSL Decryption > SSL Forward Proxy**).
83149	Fixed an issue where a missing node (*user*) in the unlock command prevented administrators from using the Panorama web interface to unlock a locked LDAP user.
83142	Fixed an issue where triggering a DHCP release did not clear the original settings for a DHCP client that was in `renew` state.
83113	Fixed an issue where attempts to regenerate metadata caused a process (*update_vld_itvl_idx*) to stop responding when encountering a corrupt log file (a log file that contained invalid data). With this fix, the metadata regeneration process skips log files that contain invalid data so that regeneration task is successfully completed.
83102	Added functionality to allow commits to succeed even when there is no Network Processing Card (NPC) installed, yet, or when the NPC is not supported or recognized in the current PAN-OS release. With this fix, you can install PA-7000 Series cards that are not supported in the PAN-OS version shipped with or running on the firewall and then upgrade to the appropriate PAN-OS version.
83041	Fixed an issue where adjustments to the width of columns in the web interface are not saved, causing columns to revert to previous settings when you view a different tab. With this fix, changes to the width of columns in the web interface are retained until changed again.
83004	Fixed an issue where a Zone Protection profile with strict IP checking enabled resulted in incorrectly dropped packets. These drops were caused by an improper check of whether the source IP address was a broadcast address.

Issue ID	Description
83001	Fixed an issue on an M-100 appliance where available disk size was reported as 0 bytes during an upgrade. This incorrectly caused old logs to be purged from the other Log Collectors in the group in an attempt to adhere to the configured log quota for the group. Additionally, Panorama 6.1.8 and Panorama 7.0.3 (and later releases) on an M-100 appliance with zero disk space displays an error when attempting to commit to Collector Group (`Failed to commit collector config`) or a warning when attempting to commit to Panorama (`Disk <disk-ID> on log collector <log-collector-id> in group <group-ID> has a size of zero bytes`).
82887	Fixed an issue where authentication attempts against a local authentication profile within an authentication sequence failed when the local profile was not the first profile in the sequence.
82853	Fixed an issue where role-based administrators were not allowed to perform API calls.
82849	Fixed an issue on a Panorama virtual appliance using a Network File System (NFS) storage partition where the file system integrity check incorrectly failed for the NFS directory, which caused the NFS mount to fail when rebooting Panorama after an upgrade to Panorama 7.0.
82838	Fixed an issue where the User-ID process (*useridd*) stopped responding when reading config messages from the Terminal Services (TS) agent.
82778	Fixed an issue where failed authentication attempts were not cleared when the authentication attempt was eventually successful. With this fix, the failed authentication attempt counter for a given user is reset as expected after every successful login.
82560	Fixed an issue where a passive VM-Series firewall in an HA pair with **Use Hypervisor Assigned MAC Address** enabled (**Device > Management > Setup**) was sending GARP requests without an established HA2 connection. With this fix, a passive VM-Series firewall no longer sends these GARP requests when you enable **Use Hypervisor Assigned MAC Address** without an HA2 connection.
82534	Fixed an issue where a firewall incorrectly injected SSL messages into traffic on port 443.
82533	Fixed an issue where the OCSP responder failed to check the validity of client certificates and showed status as `unknown` when unable to locate the custom root CA used in the certificate profile for the GlobalProtect portal configuration.
82377	Fixed an issue where, in a Large Scale VPN (LSVPN) configuration, a GlobalProtect gateway incorrectly installed the previously allocated IP address for the GlobalProtect satellite as the next hop for the routes advertised by satellites. With this fix, the GlobalProtect gateway removes any old IP addresses allocated to the satellite and correctly installs the new IP address allocated to the satellite as the next hop for the routes advertised by satellites.
82338	Fixed an issue where one-time password (OTP) RADIUS authentication failed when configured in the same authentication sequence as the domain selection. This issue was caused by the firewall incorrectly truncating the RADIUS challenge state. Also fixed OTP RADIUS authentication issues where the backslash (“\”) character was incorrectly removed from the username entry and where an incorrect password resulted in long delays before returning a password error message.
82326	Fixed an issue where additional locked users are not displayed when you click **More** in the web interface (**Devices > Authentication-Sequence > Locked Users**).

Issue ID	Description
82136	Fixed an issue where packets that matched a policy-based forwarding (PBF) rule with Action set to **No PBF** (**Policies > Policy Based Forwarding >** *pbf-rule* **> Forwarding**) were dropped when offloading was enabled. With this fix, offloaded sessions are passed as expected even when the traffic matches a PBF rule with **Forwarding** set to **No PBF**.
82109	Fixed an issue on a PA-7000 Series firewall where passive FTPS with inbound decryption failed after entering passive mode. This occurred when predict sessions did not merge as expected due to the predict queue. With this fix, proxy ingress executes before the predict queue so that all data sessions merge as expected and FTP transfer is successful over TLS.
82099	Fixed an issue where the remote host (From) IP address for the Panorama session displayed in reverse order—displayed the administrator IP address—in the Logged in Admins widget on the **Dashboard**.
81944	Fixed an issue where patch management for a GlobalProtect host information profile (HIP) check failed to identify missing patches when the Check setting for patch management in HIP Objects criteria was set to **has-all**, **has-any**, or **has-none** (**Objects > GlobalProtect > HIP Objects > Patch Management > Criteria**).
81927	Fixed an issue where a firewall stopped submitting files to a WildFire cloud (public or private) when a CPU process (*varrcvr*) stopped responding. This issue occurred when receiving an email with a subject line containing more than 252 characters.
81868	Fixed an issue with a packet buffer (*FPTCP*) leak and resolved a few dataplane-to-management plane connection issues, as well.
81584	Fixed an issue in Panorama 7.0 where output from the `show ntp` command did not always display the correct NTP status. Primarily, this issue occurred when there was only one NTP server configured and, even when correctly connected to the NTP server, the `show ntp status` displayed as `rejected`. With this fix, output from the `show ntp` command correctly displays NTP status as `synchronized`.
81581	Fixed an issue where a process (*useridd*) was unable to accommodate a large number of HIP reports during HA synchronization, which caused abnormally high CPU and memory utilization on the firewall.
81522	Fixed an issue where a firewall allowed commits to succeed even when there were no superuser administrator accounts included in the configuration. This would cause the firewall to be inaccessible (except when the firewall was managed by Panorama, which could still provide access to the firewall through Panorama context switching). With this fix, a commit succeeds only if there is at least one local superuser account in the configuration; if none exist, the commit fails.
81415	Fixed an issue on PA-7000 Series, PA-5000 Series, PA-3000 Series, and PA-500 firewalls where an Aggregate Ethernet (AE) interface was unable to transmit an ARP request on a tagged subinterface to the neighboring device.
81408	Fixed an issue where shared address objects that are not used in security policy rules were pushed to firewalls even when Panorama Settings (**Panorama > Setup > Management**) was configured to not **Share Unused Address and Service Objects with Devices**.
81383	Fixed an issue where the `show routing route` CLI command output was missing a comma ("`,`"). With this fix, the output displays correctly.
81370	Fixed an issue where the firewall was unable to allocate a large memory block, which caused sessions to fail. This fix ensures adequate resources are available for a large memory block when needed.

Issue ID	Description
81367	A security-related fix was made to address CVE-2015-4024.
81301	Fixed an issue on a firewall with decryption enabled where insufficient buffer space resulted in discarded SSL sessions.
81170	Fixed an issue where the SNMP manager returned a warning (`subtype-illegal`) related to panVsysEntry OBJECT-TYPE (panVsysName) when adding the PAN-COMMON-MIB.my MIB file. With this fix, adding the current version of MIB files to the SNMP manager does not trigger a `subtype-illegal` warning.
81079	Fixed an issue where, in a Dynamic Updates schedule pop-up (**Device > Dynamic Updates >** <*Schedule*>), hovering over the override icons displayed incorrect values for the Recurrence setting for antivirus and content updates when the Recurrence setting on the firewall was overridden by a template push. With this fix, hovering over the Recurrence value override icon for a Dynamic Update schedule displays the correct information even when the Recurrence setting was pushed to the firewall through a template push.
81058	Fixed an issue on PA-7000 Series firewalls where NAT Dynamic IP fallback did not correctly translate resources, which resulted in dropped packets.
80932	Fixed an issue where passwords for non-administrators entered in the GlobalProtect login window were truncated to 40 characters when using RADIUS authentication.
80831	Fixed an issue where SSL decryption failed for some sites when the size of the certificate was larger than 1.5KB.
80766	Fixed an issue where dataplane 0 (DP0) on the passive firewall in a high availability (HA) configuration restarted after a session was established on the active firewall interface when that same interface did not also exist on the passive firewall.
80753	Fixed an issue on a PA-3060 firewall where a network outage occurred when the number of active sessions reached 100,000. With this fix, the maximum number of detector threats (*dthreats*) is increased to avoid this issue.
80702	Fixed an issue in a high availability (HA) configuration where the ARP table synced with the primary peer but was refreshed only on dataplane 0 (DP0) of the passive peer, which caused ARP entries to expire prematurely on the passive firewall when their TTL reached 0.
80648	Fixed an issue where a device group commit failed when using the destination interface in a NAT rule configured on Panorama.
80533	Fixed an issue where administrators could view addresses and usernames in the Application Command Center (ACC) view even when the **Show Full IP Addresses** or **Show User Names In Logs And Reports** option was disabled for the Admin Role profile associated with those administrators (**Device > Admin Roles >** <*Admin Role Profile*> **> Web UI >** Privacy settings).
80463	Fixed an issue where a local commit on Panorama failed (`invalid reference`) on a template or template stack when a Log Forwarding profile was configured to send logs to syslog (**Objects > Log Forwarding**).
80397	Fixed an issue where you could create a new Monitor profile when creating a policy-based forwarding (PBF) rule on Panorama even when the target template was unknown (the PBF rule is part of a device group and the Monitor profile is part of a template configuration). With this fix, you can no longer create a new Monitor profile when creating a PBF rule on Panorama.

Issue ID	Description
80389	Fixed an issue on a PA-5060 firewall where internal packet path monitoring failed when under a heavy load. With this fix, internal packet path monitoring is forwarded using a priority setting that prevents these failures even when experiencing high traffic conditions.
80086	Fixed an issue were a firewall displayed an incorrect location for the source or destination on the Traffic Map.
79841	Fixed an issue where, in certain circumstances, there were discrepancies between a scheduled report and that same report generated using the **run now** option (**Monitor > Manage Custom Reports >** <*Custom Report*>).
79746	Fixed an issue on a PA-2000 Series firewall where an Aggregate Ethernet (AE) interface was unable to transmit an ARP request on a tagged subinterface to the neighboring device.
79328	Fixed an issue where Applications and Security rules in QoS statistics view (**Network > QoS >** <*interface*>) were not displayed when the ingress interface was configured to use L2 VLAN.
78848	Fixed a rare issue where a commit (such as an antivirus update or FQDN refresh) caused the firewall to stop processing traffic. This issue occurred after a high availability (HA) synchronization event when the autocommit triggered by the synchronization event was ignored. With this fix, a force commit request is automatically and repeatedly generated until successful.
78773	Fixed an issue where the `debug dataplane flow-control enable port` and `debug dataplane flow-control disable port` CLI commands failed to modify flow control settings as expected.
78426	Fixed an issue where a CPU process (*pan_dhcpd*) spiked when DHCP NAK packets were received on the DHCP relay interface.
78210	Fixed an issue in a high availability (HA) active/passive configuration where the multicast tree failed to converge non-offloaded multicast traffic as quickly as expected after a failover. With this fix, the multicast tree convergence time is reduced for non-offloaded multicast traffic after an HA active/passive failover.
78040	Fixed an issue where the output of the `show zone-protection zone` CLI command did not correctly display zone protection information for a defined virtual system (VSYS).
77376	Fixed an issue where a gateway Config refresh on a satellite device (**Network > IPSec Tunnels > Gateway Info** (for a *gateway*) **> select** <*gateway*> **> Refresh GW Config**) caused a delay in tunnel installation and resulted in connectivity issues for the duration of the delay.
77299	Fixed an issue where WildFire analysis reports did not display Coverage Status for the sample when using a Firefox browser even when a signature was generated to identify the sample (**Monitor > Logs > WildFire Submissions > Detailed Log View > WildFire Analysis Report**). With this fix, you can view the correct Coverage Status for a sample when using a Firefox browser.
76981	Fixed an issue where a certificate containing a space character (" ") in the Common Name field of the certificate failed to establish a secure syslog connection with the syslog server. With this fix, certificates establish syslog connections as expected even when containing space characters in the Common Name.
76811	Fixed an issue where packet loss could occur with asymmetric traffic when two PA-4060 firewalls were set up as peers in a high availability (HA) active/active configuration. This issue occurred with VLAN-tagged traffic when jumbo frames processing was disabled and large non-jumbo frames passed over the HA3 link and became jumbo frames.

Issue ID	Description
76481	Fixed an intermittent issue where a Category for a session in the URL Filtering log did not match the actual categorization of that session. With this fix, the logic for removing expired or unresolved URL cache entries is improved so that a Category in the URL Filtering log stays in sync with the actual categorization of a session.
72115	When the web interface was set to display in any language other than English, service routes to specify how the firewall communicates with other servers or devices could not be configured (**Device > Setup > Services > Service Route Configuration**). This issue has been fixed so that service routes can be configured and work correctly when the web interface is set to any language preference.
70719	In response to an issue where a dataplane restarted due to an incorrect flow ID, PAN-OS 6.1.4 and later releases included additional checks to help prevent the dataplane from restarting due to this issue. With this fix in PAN-OS 7.0.3, those PAN-OS 6.1.4 modifications are further modified to provide a more complete solution that avoids inadvertently dropping IPv4 traffic affected by this issue.
67254	Fixed an issue where an XML API call for system RAID failed with an attribute error for `raid_handler` object.
66607	Fixed an issue on a PA-200 firewall where administrators could configure a firewall directly or use Panorama to push external block lists (EBLs) with a total number of EBL lists or IP addresses that exceeded limitations and did not receive an error message. (Low-end platforms support a maximum of 10 lists and 50,000 IP addresses; high-end platforms support a maximum of 30 lists and 150,000 IP addresses; there is no per-list maximum for any platform.) With this fix, an error message is displayed as expected when configuring a PA-200 firewall directly or through a push from Panorama (or PAN-OS release downgrade) where the number of EBL lists or IP addresses exceeds the limitations of that firewall or of the current PAN-OS release.
34340	Fixed an issue where a large number of informational logs for the key manager process (*keymgr*) were included in reports when log setting for keymgr logs was set to `normal`. With this fix, informational logs for *keymgr* are included only when you configure logging for keymgr messages to the debug setting using the `debug keymgr on debug` CLI command.

PAN-OS 7.0.2 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.2 release. For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Issue ID	Description
82724	Fixed an issue where old registered IP addresses in a Dynamic Address Group on a high availability (HA) active/passive pair were deleted from the passive firewall when that firewall switched from non-functional to passive state and received an incremental update of registered IP addresses from the active firewall. This fix also addressed a related issue in an HA active/active configuration where the active-secondary firewall retained old IP addresses in the Dynamic Address Group after switching to a functional state when the active-secondary firewall switched to non-functional state and all IP addresses in the Dynamic Address Group became unregistered on the active-primary firewall.
82717	Fixed an issue where a dataplane stopped responding after a reboot due to an initialization issue on SFP+ ports.
82675	Fixed an issue on an M-100 appliance where, after an upgrade to PAN-OS 7.0.1, an authentication process (*authd*) stopped responding when the LDAP binding password contained special characters.
82370	Fixed an intermittent issue where a dataplane process (*mprelay*) experienced a memory leak that caused the virtual memory to increase until it triggered a dataplane restart.
82310	In response to a fragmentation issue, virus patterns are split into smaller chunks to reduce the possibility of memory allocation failure.
82087	Fixed an issue where a firewall displayed an alert for low disk space. With this fix, the /opt/content directory was removed to improve the disk cleanup process.
82009	Fixed an issue where a document file triggered an attempt to ping an IP address.
81981	Fixed an issue where the LLDP System Name field displayed the firewall model number and could not be modified to differentiate from other similar firewalls. With this fix, the firewall populates the LLDP System Name field using the configurable hostname value.
81970	Fixed an issue where some Active Directory (AD) servers were incorrectly displaying a `Password expires in x days` message even after selecting **Password never expires** on the AD server. With this fix, the AD server ignores the maximum password age (maxPwdAge) value when the **Password never expires** option is selected.
81955	Fixed an issue on a firewall where files were not sent to WildFire as expected when the first 8 bytes of the file were split across different packets or decrypted buffers.
81941	Fixed an issue where a dataplane restarted when encountering resumed SSL sessions using inbound SSL decryption.
81819	Fixed an issue where the System log reported that a firewall in a high availability (HA) active/active configuration `Received conflicting ARP` for the floating IP address of its HA peer. With this fix, duplicate IP address detection continues to log conflicts for non-floating IP addresses, as well as duplicate addresses detected for a floating IP address received from any other device that is not a member of the HA pair.

Issue ID	Description
81816	Removed support for SSLv3 on Panorama for connections to managed devices.
81797	Fixed an issue where ASCII and special characters were not supported in the user activity report username field.
81783	Fixed an issue where a firewall picked the wrong decryption cipher when configured with multiple IPSec Crypto profiles for IKEv2 negotiation.
81676	Fixed an issue where a firewall allowed administrators to configure subinterface with using invalid notation (such as ethernet1/1.1.1).
81577	Fixed an issue where custom URL categories associated with a Decryption policy did not match traffic destined for a proxy server.
81572	Fixed an issue on a PA-7000 Series firewall that displayed incorrect timestamps in Traffic, Threat, and URL Filtering logs.
81535	Fixed an issue where the group list was empty after pushing the group mapping configuration from Panorama to a multi-vsys firewall during an attempt to configure users in a Security policy rule even though the group mapping state was synchronized.
81510	Fixed an issue where Device Group and Template administrators were able to create and modify Shared objects. With this fix, Device Group and Template administrators are allowed to create and modify only objects specific to the device groups and templates to which they have access—not Shared objects.
81500	Fixed an issue where a VM-Series firewall in a VMware NSX configuration running on an ESXi server restarted when a process (*all_task*) stopped responding.
81485	Fixed an issue on PA-200 and VM-Series firewalls where local objects were not resolved in the Traffic log after selecting the **Resolve hostname** option (bottom of the **Monitor > Logs > Traffic** tab).
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.
81389	Fixed an issue where the output of the `show admins all` command displayed all administrator accounts on the firewall, including root accounts. With this fix, `show admins all` command output displays only local and non-local administrator accounts.
81373	Fixed an issue where WildFire Analysis reports for samples analyzed in a WildFire cloud (public or private) were not displayed in the WildFire Submissions log (**Monitor > WildFire Submissions**) when the firewall was configured to communicate with the WildFire cloud through a proxy server.
81312	Fixed an issue where firewall Device administrators were unable to run and view output on a firewall for the `show panorama-status` CLI command. With this fix, **Device administrator**, **Device administrator (read-only)**, **Superuser**, and **Superuser (read-only)** users (**Device > Administrators >** *<administrator>*) can run and view output for the `show panorama-status` command from the firewall.
81271	Fixed an issue where the second attempt to access some websites over HTTPS failed when SSL Forward Proxy was enabled.

Issue ID	Description
81264	Fixed an issue where Threat logs were generated for `Threat Name - IP fragment overlap, ID - 8705` after upgrading to a PAN-OS 7.0 release.
81219	Fixed an issue with stability when adding Log Collectors to a Collector Group.
81115	Fixed an issue where administrators experienced long delays when executing log queries consisting of multiple attributes.
81110	Fixed a session reuse issue where an incoming SYN/ACK packet for an established session caused a failure in TCP reassembly, which resulted in a dropped packet even the Reject Non-SYN TCP option was disabled (**Network > Network Profiles > Zone Protection >** *<Zone Protection profile>* **> Packet Based Attack Protection > TCP Drop**). With this fix, initiating session reuse with a SYN/ACK packet is successful regardless of the Reject Non-SYN TCP setting.
80993	Fixed an issue in PAN-OS 7.0 (as well as in Panorama 5.1 and later releases) where XML API POST requests failed when including a QUERY_STRING but no content-length header. With this fix (in both PAN-OS and Panorama 7.0.2 releases), POST requests with a QUERY_STRING and a missing content-length header are successful.
80960	Fixed an issue where attempting to **Test SCP server connection** (**Device > Scheduled Log Export**) created an unnecessary Config lock that prevented any additional changes to the running configuration.
80933	Fixed a rare issue where a PA-7000 Series firewall experienced heartbeat failures on the HA1 and HA1 backup links that caused split brain in a high availability (HA) configuration.
80924	Fixed an issue where a GlobalProtect Large Scale VPN (LSVPN) satellite configuration caused the satellite firewall to Proxy ARP for the defined access route subnets on all logical and physical interfaces.
80896	Fixed an issue where some actions that utilize the /opt/pancfg/ partition, such as dynamic updates and commits, were failing when that partition ran out of space due to a large number of HIP reports received from User-ID XML API. With this fix, HIP reports are no longer saved in the /opt/pancfg/ partition of the firewall.
80840	Fixed an issue where the URL filter did not correctly parse the common name (CN) value when a MAC address was specified as the CN value in the server certificate.
80839	Fixed an issue where `error` is displayed for Tor status in the CLI output for both the `show wildfire status` and `test wildfire tor` CLI commands.
80767	In response to a very rare issue where the configured NAT pool or method was not utilized as expected, an enhancement was made to Tech Support file generation that includes additional data to help troubleshoot the issue.
80720	Fixed an issue where a firewall experienced a dataplane restart when the packet processing daemon terminated due to a double free condition associated with a specific packet buffer (*fptcp*).
80687	Fixed an issue on PA-7000 Series, PA-5000 Series, and PA-3000 Series firewalls where software packet buffers were depleted (although eventually recovered) when receiving TCP packets with large payloads. With this fix, modifications to processes for allocating software buffers and handling TCP congestion en-sure that software packet buffers do not get depleted due to packets with large payloads.
80669	Fixed an issue on firewalls in CCEAL mode where the management server would restart when the firewall attempted to send an SNMPv3 trap.

Issue ID	Description
80624	Fixed an issue where administrators experienced delays accessing the firewall web interface when the firewall reconnected to Panorama and had a large number of logs to send.
80592	Fixed an issue where firewalls in a high availability (HA) active/passive configuration did not sync the Dynamic Address Group when one of the firewalls stopped functioning and then changed to a functional state.
80567	In response to an issue where race conditions affecting Block IP table operations inadvertently caused some packets to be marked as `drop ip block` without any entry in the Block IP table.
80532	Fixed an issue where files were not being forwarded as expected to the WildFire cloud (public or private) due to a terminated process (*varrcvr*). This issue occurred when the Subject field in forwarded emails contained non-ASCII characters.
80404	Fixed an issue where PA-2000 Series firewalls experienced connectivity issues when auto-negotiating duplex and speed settings on the management interface connection to a third-party device. With this fix, a new driver is added to ensure that the management interface remains accessible and to provide a more reliable transition when speeds are changed (such as from 1,000 Mbps over full duplex—1000/Full—to 100/Full) when there is little or no traffic flowing through the firewall. Use the following best practice recommendations to ensure successful transitions: • When possible, set both the PA-2000 Series firewall and the third-party device to auto-negotiate mode, where each side selects the highest possible common maximum speed and duplex setting. • If you must manually configure the speed and duplex setting for either the firewall (**Device > Setup > Management > Management Interface Settings**) or the third-party device, you should manually configure the same speed and duplex settings on both sides so that they are in sync. If you do not manually configure the settings to be the same at both ends of the connection, traffic flow will be impacted because the PA-2000 Series firewall cannot determine the correct duplex mode and will default to half-duplex mode, which can cause a duplex mismatch. ⚠ If you manually configure both sides of the connection: – Do not set the port on the third-party device to 1000 Mbps master mode, as this will completely stop traffic and the ports will not recover (both ports try to control the link and neither is successful). – Do not attempt to change the speed or duplex setting while traffic is flowing through the connection: pause traffic, configure the two peer ports appropriately, make sure the ports are set to the same speed and duplex values, and then resume traffic flow.
80386	Fixed an issue where a configuration override failed when pushing system log settings to firewalls from Panorama resulting in the following error: `edit failed, may need to override template object informational first.`
80318	Fixed an intermittent issue on a PA-7000 Series firewall where some packets were dropped during the initial session setup process. This issue occurred when two packets in the same session were sent almost simultaneously, causing the second of the two packets to get dropped.

Issue ID	Description
80251	Fixed an issue on a firewall where a dataplane restarted with multiple core files (all_pktproc, flow_ctrl, and flow_mgmt) after the firewall received percent-encoded HTTP requests from a proxy server when both the parsing of X-Forwarded-For (XFF) attributes and stripping of XFF from HTTP Headers were enabled (configured with the `set system setting ctd` CLI command). With this fix, you can enable both XFF actions without causing the dataplane to restart when the firewall receives percent-encoded HTTP request from a proxy server.
80187	Fixed an issue where the `test authentication authentication-profile` command results in output that uses the management interface as the source regardless whether you configured a service route to provide a different source.
80063	Fixed an issue on an M-100 appliance where the configuration daemon (*configd*) stopped responding when processing a null value.
79960	Fixed an issue where the firewall sent an extra carriage return line feed (CRLF) in HTTP/1.1 POST packets when requesting an update from the BrightCloud URL database. This issue occurred when using a proxy server, which correctly rejects the packets and returns HTTP/1.1 400 Bad Request messages due to the extra CRLF (per RFC 7230).
79929	Fixed an issue where a process (*mprelay*) stopped responding and did not receive a refresh of the configuration when it restarted.
79925	Fixed an issue where virtual wire (vwire) path monitoring failed and the firewall stopped sending ICMP packets over the vwire interface after a high availability (HA) failover.
79719	Fixed a rare issue where a dataplane restarted when multiple processes (*flow_ctrl* and *mprelay*) stopped responding due to a software buffer leak.
79709	Fixed an intermittent issue where ZIP processing may cause the dataplane to restart.
79535	Fixed an issue in a high availability (HA) configuration where the monitored destination IP address for Path Monitoring displayed as `up` even when unavailable, preventing the firewall from displaying as `tentative` as expected. With this fix, the monitored destination IP address correctly shows as `down` when unavailable, which results in the firewall correctly changing status to `tentative`.
79504	Fixed an issue where a passive M-100 appliance in a high availability (HA) configuration lost its device group and template configuration.
79470	Fixed an issue where Panorama did not display WildFire Analysis reports correctly in the WildFire Submissions log for WF-500 appliances running PAN-OS 6.1 or earlier releases. You can fetch these reports using a secure channel only for WF-500 appliances running PAN-OS 7.0.2 or later releases; a secure channel is not used when fetching reports from a WF-500 appliance running PAN-OS 7.0.1 or earlier releases.
79382	Fixed an issue where IP address registration through the XML API failed to populate the Dynamic Address Group following an `AddrObjRefresh` job failure during a template commit from Panorama when the **Force Template Values** option was checked, resulting in an `Error: Failed to parse security policy`.
79347	Fixed an issue where a firewall stopped responding and triggered a dataplane restart when receiving incomplete and insufficient parameters in API calls. With this fix, checks are in place to prevent the dataplane restart when receiving API requests with invalid or insufficient parameters.

Issue ID	Description
79279	Fixed an issue that caused an error to be displayed (`ntp-servers unexpected here. Discarding.`) when pushing a device group configuration through templates after a Panorama upgrade.
79046	Fixed an issue on an M-Series appliance running in Log Collector mode where log forwarding to an external syslog server stopped working after a Panorama commit when forwarding logs through TCP port 514 (default) instead of UDP port 514 (**Device > Server Profiles > Syslog**). With this fix, you no longer need to perform a Collector Group commit to resume log forwarding after a Panorama commit when the syslog server is configured to use TCP.
78891	Fixed an issue where the use of region-based objects in the Security policy caused consistently high dataplane CPU utilization.
78803	Fixed an issue in Panorama where template settings that were global to every virtual system (vsys) on a firewall (for example, System log settings) were unable to reference configuration elements (for example, an Email server profile) when that element was added to a specific vsys instead of to the Shared location. With this fix, Panorama can push template and device group settings—even those that are not or can't be pushed to a specific vsys—regardless whether those settings refer to Shared elements or elements that are specific to a vsys.
78571	Fixed an intermittent issue where a firewall received a Virtual Systems license that allowed for a higher number of virtual systems than the maximum amount supported for the platform. With this fix, the licensed virtual systems activated on a firewall cannot be higher than the maximum amount of virtual systems supported on the firewall.
78568	Fixed an issue where PA-3000, PA-5000, and PA-7000 Series firewalls experienced a memory leak associated with improper purging of old, replaced entries in the ARP/ND table when the table reached capacity.
78511	Fixed an issue where the DHCP relay agent incorrectly set the gateway IP address (*giaddr*) value to zero (instead of the IP address of the ingress interface as defined in RFC 1542) when responding to DHCP requests.
78084	The output for the command `show log collector serial number` displayed different log data when executed on a primary-active Panorama than the output that was displayed when the command was executed from the secondary-passive Panorama. This issue is fixed so that the output for the command `show log collector serial number` correctly displays the latest log data for managed Log Collectors.
78064	Fixed an intermittent issue where authentication failed in a two-phase authentication process when the login response contained customer data.
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.
77775	Fixed an issue where a validation error occurred when attempting to move an object from its current device group to a destination device group that was lower in the hierarchy even when the policy rules or objects that reference the object being moved were in the same destination or in a device group that should inherit the object.
77103	Fixed an issue where a System log message (`Failed to upgrade WildFire package to version <unknown version>`) displayed on the firewall even when no WildFire license existed on the firewall.

Issue ID	Description
76875	Fixed an issue where the dataplane rebooted when a process (*brdagent*) was terminated by the firewall in response to an out of memory condition. With the fix, dataplane reboots are no longer triggered by these out-of-memory events because the firewall no longer considers the brdagent process for termination when attempting to address an out-of-memory event.
76781	Fixed an issue where a firewall incorrectly calculated packet length and TCP sequence due to a one-byte zero-window-probe packet when that packet was sent from one vsys to another.
76631	Fixed an issue on PA-7000 Series firewalls where the Log Processing Card (LPC) failed to resolve the FQDN of the syslog server. With this fix, the firewall will re-initiate the DNS lookup request until the lookup succeeds.
76561	Fixed an issue where the DHCP relay agent dropped DHCPDISCOVER packets that the agent could not process due to multiple BOOTP flags. With this fix, the DHCP relay agent recognizes the first BOOTP flag in a DHCPDISCOVER packet and ignores any additional BOOTP flags that may exist (per RFC 1542) so that multiple BOOTP flags do not cause DHCPDISCOVER packets to be dropped.
76238	A security-related fix was made to address CVE-2015-1873.
75803	Addressed an issue regarding how often password API keys are regenerated.
75344	Fixed an issue where a memory process restarted and caused an invalid memory reference; the invalid memory reference resulted in a management plane restart.
74423	Fixed an issue where a firewall running PAN-OS 7.0.1 was incorrectly using the URL Updates service route when fetching a Dynamic Block List instead of using the service route attached to the Palo Alto Updates in the Service Route Configuration (**Device > Setup > Services > Global**).
73443	Fixed an intermittent issue that resulted in corrupted forwarding entries on the offload processor.
71331	Fixed an issue on a PA-500 firewall where the firewall assigned a DHCP address for the management (MGT) interface even after the administrator configured a static IP address for that port. With this fix, DHCP initiation for the MGT interface is disabled.
70887	Fixed an issue where clicking the **More** link to view the registered IP address under **Object > Address Groups** resulted in an error if the name of a Dynamic Address Group included a space. With this fix, spaces in Dynamic Address Group names no longer cause an error when displaying the IP address.
70302	Fixed an issue where the autocommit process failed after upgrading a PA-7050 or PA-5000 Series firewall to a PAN-OS 6.1 or PAN-OS 7.0 release.
69132	Fixed an issue where occasional dataplane restarts occurred due to a kernel memory allocation failure.
64602	In response to an issue where a firewall generated core files for a process (*pktproc*) when a dataplane stopped responding, an additional check and associated error output is added to help troubleshoot an issue where an FPGA running the Aho-Corasick algorithm returns a session index mapped to a NULL pointer.

Issue ID	Description
64531	Fixed an issue where a high availability (HA) failover occurred due to insufficient kernel memory on a PA-5000 Series firewall. With this fix, PA-5000 Series firewalls include some cache-flushing events and increased kernel memory to ensure sufficient kernel memory remains available for ping requests and keep-alive messages to avoid these HA failovers.
64266	Fixed a rare issue where certain processes (*l3svc* and *sslvpn*) stopped responding when a Content update and FQDN refresh occurred simultaneously.

PAN-OS 7.0.1 Addressed Issues

The following table lists the issues that are addressed in the PAN-OS® 7.0.1 release. (As the base PAN-OS 7.0 image, this release and the list below also include all issues initially addressed for PAN-OS 7.0.0.) For an overview of new features introduced in PAN-OS 7.0 and other release information, including the list of known issues, see PAN-OS 7.0 Release Information. Before you upgrade or downgrade to this release, review the information in Upgrade to PAN-OS 7.0.

Issue ID	Description
PAN-73605	Fixed an issue where the firewall did not correctly identify the URL category of a web session when the HTTP header information was split across multiple packets due to a sequence of abnormally large HTTP cookies.
82299	Fixed a critical security vulnerability for firewalls and Panorama running PAN-OS 7.0.0 that were configured to use LDAP authentication for Captive Portal or for device management. (This issue does not affect devices configured to use RADIUS or local authentication.)
81374	Fixed an issue on a PA-200 firewall where the MAC address configured for the management interface was inadvertently changed after an upgrade to PAN-OS 7.0.0. With this fix, the management interface MAC address configured before an upgrade remains the same after the upgrade.
81174	Fixed an issue where an autocommit failed after an upgrade to PAN-OS 7.0.0 due to a failed IKE Crypto profile verification when two IKE gateways were configured using a dynamic peer in `main` mode on the same local interface.
81167	Fixed an issue where the Apps-only (no Threats) version of Content Updates failed to install on a device registered with standard support.
81158	Fixed an issue where an IPSec tunnel failed to negotiate a new session and dropped packets during an SA re-key in IKEv2 mode.
81024	Fixed an issue where Panorama™ 7.0.0 failed to properly push Device Group and Service Group objects to devices running PAN-OS 6.1 or earlier releases. With this fix, Panorama pushes Device Group and Service Group objects as expected to devices running any supported PAN-OS release.
80903	Fixed an issue where PA-7050 firewalls running PAN-OS 6.1 or earlier releases did not accurately handle queries from Panorama running PAN-OS 7.0.0, which resulted in the inability to display data in the Application Command Center (ACC) widgets and prevented log data from the PA-7050 firewall from being included in reports generated on Panorama. With this fix, Panorama queries to PA-7050 firewalls are disabled by default so that ACC widgets display correctly for all other devices you manage through Panorama.
80871	Fixed an issue where WildFire™ analysis reports were not displayed in Detailed Log View (**Monitor > WildFire Submissions > Detailed Log View > WildFire Analysis Report**) for WildFire Submissions log entries when the firewall was configured to use a service route instead of the management interface to communicate either with a WildFire private cloud or with the WildFire public cloud. However, for firewalls running PAN-OS 7.0.1, to view the integrated reports from within the web interface on the firewall, you must first configure `wildfire.paloaltonetworks.com` as the WildFire public cloud; either in the web interface (**Device > Setup > WildFire > General Settings**) or using the `set deviceconfig setting wildfire public-cloud-server wildfire.paloaltonetworks.com` CLI command.

Issue ID	Description
80849	Fixed an issue where IPv4 and IPv6 traffic forwarding failed when sent through an LACP Aggregated Ethernet (AE) interface due to an incorrect system MAC address.
80799	Fixed an issue where files and email links sent using Simple Mail Transfer Protocol (SMTP) or Post Office Protocol version 3 (POP3) were not forwarded to the WildFire public cloud for analysis unless the firewall was also configured to forward files to a WildFire private cloud. With this fix, firewalls connected only to the WildFire public cloud appropriately forward to the WildFire public cloud all files and email links that are sent using SMTP or POP3.
80607	Fixed an issue where a firewall rebooted when an unusually large number of fragmented packets passed through the firewall when the **NAT64 IPv6 Minimum Network MTU** setting was configured to a value other than 1500 (**Device > Setup > Session > Session Settings**), which triggered a memory leak. With this fix, fragmented packets no longer cause a memory leak. Additionally, a new counter was to monitor whether resources are available for fragmenting packets when needed.
80561	Fixed an issue where software forwarding of Layer 3 multicast traffic with Protocol Independent Multicast (PIM) did not function properly.
80408	Fixed an issue where, in some environments, new content updates could no longer be accommodated by the memory on the firewall that is allotted for these files due to a continually increasing number of applications in the updates. With this fix, allocated memory for content updates is increased so that continued growth of content updates will not prevent successful download and installation of those updates.
80398	Fixed an issue where administrators were unable to log in through the web interface when the firewall was configured to authenticate administrators using client certificates and was configured with Online Certificate Status Protocol (OCSP) verification enabled.
80373	Fixed an issue where attempts to **Clone** objects or policies in a shared gateway location or **Move** objects or policies from a virtual system to a shared gateway location did not work correctly.
80323	Fixed an issue where the link states for firewall interfaces did not come up when rebooting the firewall after disabling high availability (HA).
80286	Fixed an issue where a commit failed after an upgrade to PAN-OS 7.0.0 when Defaults for an application was set to `ICMP Type` (**Objects > Applications > application > Advanced**). With this fix, commits do not fail after an upgrade to PAN-OS 7.0.1 or later releases regardless of this Defaults setting.
80268	Fixed an issue on a PA-7050 firewall running PAN-OS 7.0.0 where attempts to switch to Common Criteria (CC) mode failed with the following error: `Set CCEAL4 Mode Sysd Error.` This issue occurred because the CC mode operation attempted to change the operational mode before the system process (*sysd*) was fully loaded. This operation resulted in setting the firewall to the factory default configuration without CC configuration changes.
80266	Fixed an issue where PA-200, PA-500, and PA-2050 firewalls running PAN-OS 7.0.0 and configured to use a service route instead of the management (MGT) interface to connect to an LDAP server were unable to establish a connection, which caused all firewall functions that relied on that connection to fail. With this fix, firewalls successfully connect through a configured service route to an LDAP server.
79854	Fixed an issue where Panorama was unable to display System and Config logs for PA-7000 Series firewalls.

Issue ID	Description
79844	Fixed an issue where logs sent to a log collector group were not properly saved and could not be displayed when that log collector group contained a space in the name. With this fix, logs are saved and displayed correctly even when there is a space in the log collector group name.
79522	Fixed an intermittent issue where a firewall with hardware offload enabled included an incorrect IP checksum value in outgoing NAT packets, which caused some packets to be dropped.
79511	Fixed an issue on Panorama where disabling the **Share Unused Address and Service Objects with Devices** option (**Panorama > Setup > Management > Panorama Settings**) when no Shared objects were configured caused a process to restart during a commit.
79478	Fixed an issue where the firewall connected directly to a directory server instead of the User-ID agent configured as an LDAP proxy. With this fix, the firewall correctly uses the User-ID agent when the agent is configured for use as an LDAP proxy.
79463	Fixed an issue where CPU memory on a PA-7050 firewall spiked when attempting to view reports in the Application Command Center (ACC). This issue occurred when task creation notifications were not processed properly and, as a result, the Log Collector did not terminate failed requests as expected. With this fix, task creation notifications are processed appropriately and failed tasks are properly terminated.
79443	Fixed an issue in the web interface where, in some cases, the PHP session cookie (`PHPSESSID`) was not marked as secure.
79401	VM-1000-HV firewalls running on eight vCPUs did not save and display Traffic and Threat logs. With this fix, VM-1000-HV firewalls properly save and display the logs. This issue did not affect VM-Series firewalls running on two or four vCPUs.
79367	Fixed an issue in PAN-OS where GlobalProtect™ clients experienced delays and intermittently failed to retrieve the gateway configuration for connecting to a GlobalProtect gateway when the firewall was in a high availability (HA) configuration and under a heavy load. This issue occurred due to an issue with the synchronization of HIP reports between gateways on HA peers when there was a high number of near-simultaneous GlobalProtect connection requests. With this fix, the sync process is modified so that GlobalProtect clients are able to download the configuration and connect to the network as expected even when multiple clients are attempting to connect at the same time.
79335	Fixed an issue where attempting to filter System logs using the log filter `Type equal globalprotect` did not work. A space was automatically added to the log filter, causing an error to be displayed.
79291	Fixed an issue where the Bytes column results displayed when clicking **Run Now** for a custom report (**Monitor > Manage Custom Reports**) did not match the results displayed in that same report when emailed or exported out in PDF format.
79278	Fixed an issue where the active device in a high availability (HA) configuration failed to generate tech support files due to a buffer limitation that could not accommodate the output from some commands. With this fix, the commands that prevent generation of tech support files have been removed so that reports are generated as expected.
79260	Fixed a rare issue on a WF-500 appliance where an ICMP packet containing a FIN+ACK packet was incorrectly forwarded out through the management (MGT) interface. With this fix, ICMP packets containing a FIN+ACK packet are dropped, instead.

Issue ID	Description
79104	Fixed a rare issue on a PA-7000 Series firewall where the HA1 and HA1 backup links experienced heartbeat failures that caused split brain in a high availability (HA) configuration.
78798	Fixed an issue where the URL field in the URL Filtering log became blank or was logged without a hostname.
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.
78646	Fixed an issue where a firewall replaced multibyte characters with a period character (`.`) when forwarding logs or event information to SNMP traps, to a syslog server, through email, or in scheduled log exports. This issue also occurred when exporting logs to CSV. With this fix, multibyte characters are forwarded and exported correctly with one exception: in PAN-OS 7.0.1, PA-7000 Series firewalls will still incorrectly replace multibyte characters with period characters when exporting logs to CSV.
78621	Fixed an issue that occurred when Chile adopted new official times and the official time for Continental Chile became UTC-03:00. A PA-200 firewall configured to use the Chile Continental time incorrectly continued to display the official time as UTC-04:00.
78556	Fixed an issue in Panorama where using the option to import a certificate when configuring a GlobalProtect gateway or portal did not result in the imported certificate being added to the drop-down. The imported certificate also did not display on the **Templates > Device > Certificates** page. (However, the imported certificate did display correctly after a Panorama commit.) With this fix, imported certificates are displayed immediately on the web interface where expected.
78448	Fixed an issue where a custom response page containing an invalid substring caused the process for communicating between the dataplane and management planes (*mprelay*) to stop responding when attempting to commit configuration changes.
78436	Fixed an issue where the management plane stopped responding when more than one process attempted to modify the device table during a configuration push from Panorama™. With this fix, the device table is locked and modifiable by only one process at a time to avoid conflicting modifications.
78413	Fixed an issue on a PA-7000 Series 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.
78343	Fixed an issue that occurred with decryption enabled, where some websites were not decrypted due to an issue with certificate serial numbers.
78304	A security-related fix was made to address a cross-site request forgery (CSRF) issue in the web interface.
78289	Fixed an issue where the `receive errors` interface counter displayed values larger than the actual number of packets that should be counted as errors. This issue occurred because some packets were counted twice. With this fix, the `receive errors` counter displays the correct value.
78197	HIP reports for users can now be retrieved using the XML API (in addition to viewing HIP reports using the CLI).

Issue ID	Description
78187	Fixed an intermittent issue with a system process (*all_task*) that caused a device to restart unexpectedly. This fix includes an adjustment to an internal timer to avoid these restarts.
78166	Fixed an issue where the VirusTotal link in the Coverage Status section of WildFire™ Analysis reports did not correctly open the VirusTotal page.
78155	Addressed an issue where two DoS protection policy rules that were not overlapping incorrectly resulted in a warning that one of the rules was shadowing the other rule.
77907	Fixed an issue where log forwarding to a Log Collector did not stop as expected when executing the `request log-fwd-ctrl device <s/n> action stop` CLI command on Panorama. With this fix, log forwarding to a Log Collector stops as expected when executing the `request log-fwd-ctrl device <s/n> action stop` command so long as both the firewall and Panorama are running PAN-OS 7.0.1 or later releases.
77784	Fixed an issue on Panorama where administrators were unable to filter Device Groups by tags in the commit window.
77749	Fixed an issue where clicking **More** to view the registered IP address under **Policies > Security > Object > Address Groups** resulted in an error.
77721	Fixed an issue on a PA-200 firewall where a reboot took much longer than expected (more than 20 minutes). This issue occurred when the Content Updates database was corrupted and updates did not stop or pause as expected to allow the reboot to take place. With this fix, the firewall reinitializes the database if it is corrupted to allow the Content Update and system reboot to proceed as expected.
77477	Fixed an issue where a user was no longer able to connect to a VM-Series firewall configured as a GlobalProtect gateway and deployed in Amazon Web Services (AWS) after the user had been connected for several hours and the user could not reconnect until the gateway was restarted. With this fix, users no longer lose their connection to the GlobalProtect gateway if they stay connected for several hours.
77413	Fixed an issue where the authentication process failed to parse the base Distinguished Name (DN) correctly when it contained a space (" ") character.
77342	When using the XML API to retrieve HA control-link statistics, the statistics retrieved were not the same as those displayed in the output for the CLI operational command `show high-availability and control-link statistics`.
77307	Fixed an issue where the CLI seemed unresponsive after running the `show config diff` command due to the extended period of time it took to process and return results for a diff containing a large number of configuration changes. With this fix, the `show config diff` command returns results without any significant delay.
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.
77140	Fixed an issue where an error was displayed when using Panorama to change a password for a managed firewall admin.
76847	Fixed an issue where IKE phase 2 re-key was happening too frequently for an IPSec site-to-site VPN configured with tunnel monitoring on multiple Proxy IDs when QoS was enabled.

Issue ID	Description
76759	Fixed an issue where an SSL scan of a WF-500 appliance returned SSLv3 connections and RC4 ciphers even though the WF-500 appliance no longer supports SSLv3. With this fix, the WF-500 appliance returns only TLSv1 connections.
76729	Fixed an issue where the response returned by the `request batch license info` XML API request was not wrapped with `<response> <result>`.
76688	Fixed an issue where the IPv6 source address was not displayed in the Host column for Config logs. With this fix, the IPv6 source address is displayed in the Host column as expected (instead of 0.0.0.0).
76575	Fixed an issue on a PA-5000 Series firewall where an occasional inconsistency in the IPv6 neighbor cache on different dataplanes caused IPv6 traffic sent to certain hosts to get dropped. With this fix, the firewall keeps the IPv6 neighbor cache in sync between dataplanes so that IPv6 packets are not dropped.
76489	Fixed an issue where threat updates did not install correctly after adding a Threat Prevention license and installing an Applications and Threats content release version. This occurred even though the output of the `show system info` CLI command verified that the Threat Prevention license was installed.
76282	Fixed an issue where FQDN objects were not resolved when all the following conditions were true: • The FQDN object was being used as a tag in a Dynamic Address Group. • The Dynamic Address Group was not a member of the same tag. • The FQDN object was not attached to a security policy rule. • The FQDN object was not included in a regular address group that was attached to a security policy rule.
76083	Fixed an issue where no System logs were generated for failed login attempts using the CLI over an SSH connection. With this fix, additional System logs now provide visibility for failed logins to the management interface even if those attempts come from a CLI over an SSH connection.
76079	Fixed an issue on PA-7000 Series firewalls where Traffic logs on Advanced Mezzanine Cards (AMCs) could not be recovered after installing the AMCs onto a new Log Processing Card (LPC). With this fix, a new CLI command (`request metadata-regenerate slot <slotnum>`) is available for retrieving logs from the old AMC disks after installing them in a new LPC. When you use this command, you should ensure the device is not processing traffic until the regeneration request is complete. Additionally, you can ignore the erroneous error message (`Failure communicating with given slot`) that displays 60 seconds after running the `request metadata-regenerate` command: the regeneration process will continue to run as expected and you will need to wait for it to finish before resuming traffic flow. It can take up to two hours, or longer, to regenerate all metadata depending on the number of logs recovered. To determine if regeneration is complete, use the following CLI command to look for the `Done generating metadata for LD:x` message: `less s8lp-log vld-<amcslotnum>-0.log`
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.

Issue ID	Description
75825	Fixed a rare issue on a PA-5000 Series firewall where a race condition occurred between dataplanes 1 and 2 (DP1 and DP2) and dataplane 0 (DP0) that incorrectly caused a reset of the timeout value for parent sessions owned by DP1 and DP2 when creating predict sessions, which caused those parent sessions to time out prematurely. With this fix, the timeout for parent sessions is not changed when the predict sessions are created.
75758	Fixed an issue where the dataplane restarted on a PA-5000 Series firewall in a high availability (HA) cluster due to corruption of ARP packets.
75744	Fixed an issue where a dataplane stopped responding after a commit that changed the interface index when high availability (HA) session packets were referencing that interface index using an interface pointer.
75677	Fixed a Panorama issue where clearing the setting **Require SSL/TLS secured connection** for a vsys-specific LDAP server profile (**Templates > Device > Server Profiles > LDAP**) displayed an error.
75404	Fixed an issue for the `show log` CLI command, where you could not filter the displayed logs by username if the user/srcuser option used characters other than an alphanumeric character, underscore, dash, dot, forward slash, or colon.
75003	Fixed an issue where only the first 15 characters of a zone name was displayed in logs. Complete zone names are now displayed in logs.
74654	Fixed an issue on an M-100 device where an attempt to download Content Updates failed due to a lack of disk space. This issue occurred when continuous XML API queries filled the `/opt/pancfg` partition because STOP messages were getting dropped between Panorama and the Log Collector and queries were not properly removed when no longer needed. With this fix, STOP messages should not be dropped. Additionally, in case STOP messages are dropped for any other reason, a timeout setting for queries is in place to ensure that stale queries are removed from disk space before causing a storage space issue.
74609	Fixed an issue on a PA-5000 Series firewall where PREDICT sessions were handled by dataplane 0 (DP0) but the SIP parent sessions were on a different dataplane. With this fix, you can use the `set session filter-ip-proc-cpu dest-ip <IPaddr>` CLI command to specify all destination SIP proxy IP addresses in a filter list on the firewall. You can then use the list to configure the firewall so that DP0 receives and handles any inbound packet that is destined for any of the specified SIP proxy IP addresses.
74600	A security-related fix was made to the OpenSSL package to address multiple vulnerabilities impacting the OpenSSL libraries.
74489	Fixed an issue with regular expression where using the vertical bar or pipe character (|) caused errors.
74315	Fixed an issue where comments added to an Aggregate Ethernet (AE) interface were not saved along with the AE interface configuration and the **Comment** field displayed as empty after closing the configuration window.
73692	Updated an error message that originally noted that an Antivirus content download failed because an Antivirus content download was in progress. The error message is updated to correctly state that the failed Antivirus content download was due to a WildFire content download being in progress.
73631	Fixed an issue where several NTP sync errors were displayed following a firewall software upgrade.

Issue ID	Description
73317	Fixed an issue where the System log displayed an IPv4 address for a firewall that was connected to an Active Directory (AD) server through a management port using an IPv6 address. For example: `ldap cfg <group_name> connected to server <IPv6 address>, initiated by: <IPv4 address>`. With this fix, the appropriate IP address and format is displayed for the initiating device even when connected using an IPv6 address.
73158	The port range you can use to define ports for custom applications has been updated to be from port 0 - 65535. The update matches the ports you can define for application override policy rules (also 0 - 65535). Previously, you could not define port 0 for custom applications.
73064	When a firewall was configured as a DHCP client, it failed to renew or release the DHCP-assigned IP address when the firewall interface was then connected to a new DHCP server.
73058	Fixed an issue where source and destination fields in SNMP traps were not populated for traffic using IPv6 addresses. With this fix and Rev. B of the PAN-OS 6.1 Enterprise SNMP MIB modules, new IP version-neutral fields were added (InetAddress and InetAddressType in place of the IpAddress field) to fully support IPv6 addresses. (The IpAddress field is retained for backward compatibility but is deprecated; administrators are expected to transition to the new fields.)
72933	Fixed an issue where Panorama administrators were unable to view the Botnet report option when switched to the firewall context.
72806	The GlobalProtect™ pre-logon connect method did not work when a certificate profile was configured to use a subject alternative name (SAN) and the matching device certificate did not contain the SAN.
72756	Fixed an intermittent issue where a race condition caused by multiple processes asynchronously attempting to retrieve the last saved configuration file caused Captive Portal or the FQDN refresh job to fail.
72719	Fixed an issue where the Tunnel Monitor Threshold value displayed for a GlobalProtect satellite was incorrectly displayed as a unit of time (seconds). The Tunnel Monitor Threshold actually specifies the number of heartbeats to wait for before the firewall takes specified action, and is no longer displayed in seconds.
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.
72371	When a custom QoS profile was enabled on an interface, the QoS statistics for the custom profile were instead displayed as the default QoS profile statistics. This issue has been resolved so QoS statistics are displayed correctly with the corresponding QoS profile (and for each class in the profile).
72153	Fixed an issue where the first SYN packet in a TCP connection that passed through two virtual systems did not reach the destination server. This occurred when: • The first virtual system was configured with DNAT. • The second virtual system was configured with SNAT. • Sessions were allocated on different dataplanes (DPs), with the first session on DP0.
72075	When the firewall was configured to access an LDAP server through a data interface, the firewall could not connect to the LDAP server if it was also configured to access the User-ID agent using a different data interface.

Issue ID	Description
71860	Addressed an issue where configuration changes were not reflected in the configuration logs after importing SSH keys.
71682	Fixed an issue on a PA-5000 Series device where a port that was in use was sometimes re-used when dynamic port translation was enabled with NAT and sessions were initiated on different dataplanes. With this fix, Active FTP sessions succeed with a NAT policy setup.
71340	Fixed an issue where firewall administrators were unable to clone any of the three predefined common criteria admin roles; attempting to do so resulted in an error.
71250	Fixed an issue where decryption policies with a destination address and a URL category defined as matching criteria caused commit failures.
71049	Made an update to ensure that the CLI command `request system shutdown` can only be executed by users with superuser access privileges.
70537	Added a new debug CLI command (`debug dataplane internal pdt pci list`) to provide a dump of the peripheral component interconnect (PCI) when attempting to identify the root cause for the `data_plane_X: Startup Script Failure` error.
70431	Fixed an issue where a custom URL category with the name any caused unexpected results. With this fix, the name any is no longer allowed when creating a custom URL category (**Objects > Custom Objects > URL Category**).
70335	Fixed an issue where access routes from the GlobalProtect gateway could not be installed on a satellite when the tunnel monitor was enabled for a Large Scale VPN (LSVPN) and the tunnel monitor was in `wait recover` mode.
69961	Fixed an issue where Panorama and a firewall running the same release version, did not display the same drop-down selections to add as matching criteria to a security policy rule. Now, if Panorama and a firewall are running the same release version, the same objects are displayed and can be added to a security policy rule, regardless of whether the rule is being defined on Panorama or a firewall.
69752	Fixed an issue where the web interface did not display concurrently logged-in administrators if those administrators had not locally authenticated to the firewall.
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.
69419	Fixed an issue that was seen with predict sessions when traffic traversed a firewall in virtual wire mode twice.
68508	Fixed an issue where the DHCP server sent DHCP lease offers on the wrong interface after a high availability (HA) failover due to interface IDs being out-of-sync on the HA peers.
68484	If the Panorama setting to **Share Unused Address and Service Objects with Devices** was enabled, committing changes to a device group did not correctly push objects to managed firewalls.
68178	When configuring a threat exception for an Anti-Spyware or Vulnerability Protection profile, adding an IP address exemption to the exception did not work if the input included a subnet (for example, `XXX.XXX.XXX.XXX/32`). Only IP address exemptions entered without a subnet were accepted by the firewall. This issue is fixed so that you can add an IP address with a subnet as an exemption within a threat exception (**Objects > Vulnerability Protect/Anti-Spyware > Exceptions**).

Issue ID	Description
67713	An administrator was allowed to downgrade the content version (Applications and Threats) on the firewall to a version that was not supported with the PAN-OS software release version running on the firewall. For example, if the firewall was running PAN-OS 7.0 and the minimum content version was 497, the administrator was incorrectly able to downgrade to a version prior to 497.
66681	Resolved a dataplane restart issue due to race conditions.
65959	Added an enhancement to display predefined URL categories in addition to custom URL-categories in the Allow Categories column for URL Filtering profile rules (**Objects > Security Profiles > URL Filtering**).
63652	Fixed an issue where some files forwarded to WildFire were not uploaded successfully due to a `CANCEL_OFFSET_NO_MATCH` error. With this fix, the offset (caused by a buffer overload) is no longer an issue.
63524	Fixed an issue that occurred when performing a template commit to a PA-200 firewall on Panorama. The operation failed if you changed the vsys1 display name on the firewall using the `set display-name <name>` CLI command.
62276	Fixed an issue where the Application Command Center (ACC) failed to load any widgets and displayed the following error: `The selected filters cannot be applied to any of the acc reports.` This issue occurred when navigating from **Monitor > Reports > HTTP Applications** to the ACC.
61259	Removed white space preceding a response that was displayed when using the XML API to submit a file for WildFire analysis.

Getting Help

The following topics provide information on where to find 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 an M-Series appliance for centralized administration of the Palo Alto Networks firewalls.
- WildFire Administrator's Guide—Provides steps to set up a Palo Alto Networks firewall to forward samples for WildFire™ Analysis, to deploy the WF-500 appliance to host a WildFire private or hybrid cloud, and to monitor WildFire activity.
- VM-Series Deployment Guide—Provides details on deploying and licensing the VM-Series firewall on all supported hypervisors. It includes example of supported topologies on each hypervisor.
- GlobalProtect Administrator's Guide—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.
- Compatibility Matrix — Detailed reference to determine support for Palo Alto Networks firewalls, appliances, agents, and OS releases.
- Open Source Software (OSS) Listings—OSS licenses used with Palo Alto Networks products and software:
  - PAN-OS 7.0
  - Panorama 7.0
  - WildFire 7.0

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-support

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: June 6, 2017